HP Medical Archive Solutions
User Guide

February 2005 (Second Edition)
Part Number 389638-002

© Copyright 2005 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Bycast® and StorageGRID™ are trademarks of Bycast Inc. Their related marks, images, and symbols are the exclusive properties of Bycast Inc.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

This product includes software developed by the OpenSSL Project for use in the Open SSL Toolkit. (http://www.openssl.org/)

HP Medical Archive Solutions

February 2005 (Second Edition)
Part Number 389638-002

DISCLAIMER

While every reasonable effort has been made to achieve technical accuracy and completeness, information in this document is subject to change without notice and does not represent a commitment on the part of Bycast Inc., or any of its subsidiaries, affiliates, licensors, or resellers. There are no warranties, express or implied, with respect to the content of this document.

Features and specifications of Bycast® products are subject to change without notice.

This manual contains information and images about Bycast Inc., its fixed content storage systems, and its other products that are protected by copyright and furnished under terms of a license agreement.

This product includes software developed by the OpenSSL Project for use in the Open SSL Toolkit. (http://www.openssl.org/)

Copyright ©2005 by Bycast Inc. All rights reserved.

Proprietary and Confidential

Bycast® and StorageGRID™ are trademarks of Bycast Inc. Their related marks, images, and symbols are the exclusive properties of Bycast Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

Adobe® and Acrobat® are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

All other brands, product names, company names, trademarks, and service marks are the properties of their respective owners.

Contents

Preface . . . . . **ix**

Purpose ix

Currency ix

Intended Audience x

References xi

Document Structure xi

Using this Guide xi

Conventions xii

Contacts xiv

Getting Started **1**

Architecture Overview 2

Role of the Network Management System (NMS) . . 3

Network and Element Terminology 3

Capabilities 4

Software Requirements 5

Accessing the NMS 5

Log in 6

Log Out 6

Managing User Accounts 7

Account Management Configuration 8

Editing Your Account 10

Interface Components **11**

Frames 12

Header 12

Refresh Time 13

System Status Indicator 14

Account Management Button 14

Logout Button 14

Version Information 14

Navigation Tree 15

Tree Structure 15

Status Indicators 16

Content Frames 16
Tabs 16
Property Information (Overview) 17
Alarms 19
Reports 19
Configuration 19
Navigating Locations and Nodes 21
Location and Node Maps 21

Alarms 25

System Status Overview 26
System Monitoring 26
Notifications 27
Indicators and Propagation 28
Alarm Levels and Indicators 28
Alarms Tab 30
Main Page 31
History Page 32
Alarm Handling 34
Tracing the Source of an Alarm 34
Resolving Alarms 35

Reports 37

Introduction to Reporting 38
Accessing Reports 39
Immediate Reports 39
Quick Reports 40
Custom Reports 41
Report Formats 42
Charts 42
Text Reports 44
Chart View Controls 45
Window 45
Printing Charts and Reports 46

Services and Components 49

Overview of Services and Components 50
Services 50
Service Components 51
Interpreting Attribute Description Tables 54

ADC—Administrative Domain Controller 56
ADC Attributes 56
ADC Components 59
AMS—Audit Management System 61
AMS Attributes 61
AMS Components 64
CLB—Connection Load Balancer 67
CLB Attributes 67
CLB Components 70
CMN—Configuration Management Node 76
CMN Attributes 76
CMN Components 79
CMS—Content Management System 94
CMS Attributes 94
CMS Components 96
FSG—File System Gateway 102
FSG Attributes 103
FSG Components 105
LDR—Local Distribution Router 115
LDR Attributes 115
LDR Components 119
NMS—Network Management System 132
NMS Attributes 132
NMS Components 135
SSM—Server Status Monitor 138
SSM Attributes 138
SSM Components 140

Configuration 151

Introduction to Configuration 152
Alarm Configuration 153
Configuration—Notification Page 153
Active Alarms 155
Changing Alarm Settings 157
Service and Component Configuration 158
Configuration—Main Page 158
ADC Configuration 159
ADC Components 159
AMS Configuration 160
AMS Components 160

CLB Configuration 160
CLB Components 160
CMN Configuration 161
CMS Configuration 162
CMS Components 162
FSG Configuration 162
FSG Components 162
LDR Configuration 164
LDR Components 164
NMS Configuration 168
NMS Components 168
SSM Configuration 168
SSM Components 168

Troubleshooting Alarms 171

Overview 172
Alarm Reference Table 172

Introduction to Server Manager 195

Overview of Server Manager 196
Services 196
Capabilities 197
Architecture Overview 197
The Core Application 197
Automatic Startup and Shutdown 198

Server Manager Operation 199

Display Components 200
Header 200
Service List 201
Control Buttons 202
Server Identification 202
Prompt Line 203
Using the Interface 203
Display Updates 203
Keyboard Input 203

Command Operations 204
Monitoring Services 204
Starting Services 205
Stopping Services 205
Restarting the Server 205
Shutting Down the Server 206

Glossary 207

Index 213

Preface

Purpose

This guide is intended to familiarize you with operating the HP Medical Archive grid software. There are two software components covered by this document:

- Network Management System (NMS): the grid monitoring and reporting interface
- Server Manager: used on all servers in the HP Medical Archive

Network Management System (NMS)

Once familiar with the NMS functionality, you can routinely refer to this guide for information about system attributes, appropriate alarm responses, and configuring components and alarm notifications. The various grid service components, their configuration, and alarms are documented. An alarm troubleshooting table is included for reference.

Server Manager

This guide covers the application interface, service monitoring functionality, and application features. The objectives of this document are to enable you to use the Server Manager to:

- Monitor service operation
- Stop and start services on a node
- Restart a server
- Shutdown a server

Currency

Content of this guide is current with **release 5.2** of the HP Medical Archive software.

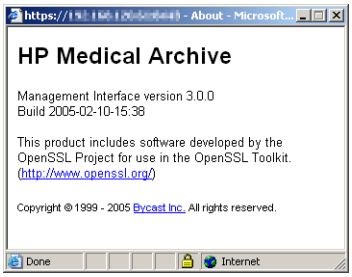
Server Manager

This release uses the Server Manager software **version 2.0**. This version of the application does not report its version number.

Network Management System (NMS)

The content is current with the NMS software release **version 3.0.0**. To find the version number of your NMS software:

1. Within any page of the NMS interface (after login), click the HP logo in the top left corner to open a dialog showing the version information.



2. Use your operating system's window close button to close the About dialog.

If you have an earlier version of NMS, contact HP technical support.

Intended Audience

The content of this guide is intended for storage grid administrators, PACS administrators, and technical support staff responsible for maintaining the HP Medical Archive system.

You are assumed to have a general understanding of the grid's components and functionality. A fairly high level of computer literacy is assumed, including knowledge of file systems, tree-structured hierarchies, and network connectivity. You should also be familiar with using and navigating an Internet web browser.

References

This document assumes familiarity with many terms related to computer operations and network administration. There is also a wide use of acronyms. An abbreviated glossary is included at the back of this guide (page 207).

Document Structure

PDF editions include hyperlinks to assist navigating the document.

You may print copies of the PDF editions for internal use but all copies must be treated as proprietary and confidential; *not* for general distribution.

Using this Guide

This guide is comprised of nine chapters covering both general information and reference tables.

Readers new to the HP Medical Archive system should read the first four chapters to gain an understanding of how the NMS works to help you monitor the grid. The first two chapters introduce the basic functionality and interface layout of the NMS. The next two chapters explain NMS functionality for understanding alarm monitoring and notifications, and for obtaining reports.

The remaining chapters provide references to look up specific information. Chapters 5 and 6 provide reference information on services and components. Chapter 7 is the final chapter on the NMS; a reference of alarms with troubleshooting tips.

The last two chapters deal with the Server Manager application used on the HP Medical Archive cabinet console(s).

Chapters

Below is a brief overview of the content of each chapter.

Chapter 1: “Getting Started”—Introducing the HP Medical Archive architecture and the role of the Network Management System within

it. This also describes the procedures to access the NMS and manage user accounts.

Chapter 2: “Interface Components”—Describing the interface components, their use, and navigation.

Chapter 3: “Alarms”—Providing a conceptual overview of NMS alarms, their types and levels, and explaining how to display, trace, and respond to alarms. Use of the alarm history is also discussed.

Chapter 4: “Reports”—Explaining the report options and formats, how to generate and print reports, and customizing the report view for the data needed.

Chapter 5: “Services and Components”—Providing a detailed reference of services, their components, and attributes.

Chapter 6: “Configuration”—Describing procedures for customizing the alarm notification settings, and other elements of system configuration.

Chapter 7: “Troubleshooting Alarms”—Providing a detailed table for administrators to locate the appropriate response to an alarm, and better understand the alarms and attributes.

Chapter 8: “Introduction to Server Manager”—Describing the Server Manager application used on the console of each server in the grid.

Chapter 9: “Server Manager Operation”—Describing procedures for using the Server Manager to gracefully connect and disconnect grid nodes.

Conventions

This guide adheres to conventions for terminology to avoid confusion or misunderstanding. There are also conventions for typography to enhance readability and usefulness of the text.

Terminology

There is some room for confusion between common computer network terminology for “server” and “node” as they are used in this document.

A server is usually thought of as a piece of computing hardware that provides data services to requesting network clients; a resource pro-

viding network, computational, and storage services. Within the context of the HP Medical Archive, a server is a piece of hardware that hosts one or more grid services.

Nodes in a network are usually defined as an independent entity with a unique network identity, running on a resource. In this text, the use of the term “node” refers to the logical entity of a building block within the HP Medical Archive; it is a server combined with a pre-defined set of grid services that perform one or more tasks within the grid.

The term “node” also appears within the NMS interface. In that context, it generally refers to a single grid service, regardless of how many services may be hosted on the server. See “Network and Element Terminology” on page 3 for additional information.

Numerics

Numeric values are presented in decimal unless noted otherwise.

Hexadecimal values in the text are noted using the prefix “0x”; for example: 0x3B.

Fonts

To assist you in easily picking out the elements of importance, changes from the standard font are used:

- Items upon which you act are shown in bold. These include:
  - Sequences of selections from the navigation tree, tabs, and page options, such as: **CN1-A-1 ▶ CMS ▶ Reports ▶ Chart**.
  - Buttons or keys to click or press, such as **Apply** or **<Tab>**.
  - Radio buttons or check buttons to enable or disable, such as **Save configuration as default**.
- Field prompts, names of windows and dialogs, messages, and other literal text in the interface is shown in sans-serif such as the LDR State pull-down menu, or the Sign In... window.
- Items within the narrative that require emphasis appear in *italics*.
- Command or parameter text that is variable (to be replaced by specific values by the system or when entered) is noted in italics, such as HPMA_GID_*<nnnn>*.

Keyboard Input

Keyboard keys that use words or standard abbreviations are shown within angle brackets, such as <Ctrl> for the control key, <Tab>, <space>, and <Enter>. Where combinations are to entered, they are noted as **<Alt>+<F7>**. Where key sequences are needed, they are noted without the plus "+", for example: **<space>Y<Enter>**.

Instructions for keyboard entry come in three forms:

- "Enter" a command or value does not specify pressing <Enter> at the end; pressing **<Enter>** at the end is assumed.
- "Type" a string or value explicitly *includes* any terminating **<Enter>** or **<Tab>** keystroke. If one is not shown, do *not* assume one.
- "Press" a key intends that only the specified key should be pressed; do not also press the <Enter> key.

Color

Color plays a helpful role in identifying elements in the text. This guide is available in color in the PDF edition. The narrative does not assume that you are reading it in color.

Contacts

For general product and company information, refer to the HP web site at:

www.hp.com

If you cannot find the information that you need in this document, there are several other resources that you can use to get more detailed information.

- The HP website (http://www.hp.com)
- Your nearest HP authorized reseller (for the locations and telephone numbers of these resellers refer to the HP website)
- HP technical support:
  - In North America, call 1-800-652-6672.
  - For other regions, refer to the HP website.

Getting Started 1

NMS and the HP Medical Archive Architecture

Elements of the grid and capabilities of the Network Management System.

Chapter Contents

Architecture Overview 2
Network and Element Terminology 3
Capabilities 4

Software Requirements 5

Accessing the NMS 5
Log in 6
Log Out 6

Managing User Accounts 7
Account Management Configuration 8
Editing Your Account 10

Architecture Overview

The HP Medical Archive architecture provides a secure, reliable, and high performance solution for the storage and distribution of very high volumes of fixed content health care data within a data center and optionally a disaster recovery (DR) site.

The term "grid computing" is inspired by the success of the interconnection of the electric power and communication network infrastructure in the late 1800s and early 1900s.

The power grid manages the available power resources and balances loads to ensure continuous operation. How and where the power originates is transparent to the consumer. During peak hours, available resources are automatically balanced and power is rerouted to where it is needed most. As demand increases, additional generating resources come online, and they are transparently utilized. Similarly, when stations go offline or get decommissioned, there are no consumer service disruptions. The grid automatically balances the available resources to changing demand; loss of a subset of resources does not result in degraded service.

Grid computing is based on the principle that access to computational resources (storage, processing power, and data) can be enhanced with high levels of reliability and scalability, analogous to obtaining electric power from the power grid. Grid storage is the application of grid computing principles to storage architecture: directories, query, resource management, and fault management.

The HP Medical Archive system is composed of multiple nodes, which form a unified archive. Each node consists of software services operating on a server that manages a limited capacity storage resource.

Within a given facility, all nodes are interconnected using standard TCP/IP networking, and communicate with local imaging modalities, PACS, and workstations. Wide Area Network (WAN) links extend the grid, enabling off-site replication of content for disaster recovery.

The HP Medical Archive deployment relies on open standards for interoperability with external hospital systems. Exchange of clinical data with external clinical systems, including PACS, viewing workstations, and modalities, takes place over standardized network file system protocols (NFS/CIFS) or (optionally) via established imaging protocols, including DICOM.

Role of the Network Management System (NMS)

The Network Management System (NMS) performs two primary functions for HP Medical Archive deployments:

- It is a monitoring system that notifies administrators of problems when the status of key hardware or software changes.
- It is a browser-based interface making the system easily available to multiple users for:
  - Reporting status information about the grid's hardware and software so you can monitor and resolve grid issues.
  - Creating, viewing, and printing reports on current and historic data about each grid component based on your selection of report criteria.
  - Configuring grid components and customizing the notification settings according to your criteria.

Network and Element Terminology

The Network Management System views the HP Medical Archive system as having tiers, or layers of detail. From the highest (big picture) to the lowest (most granular detail) the elements are:

- Locations
- Nodes
- Services
- Components
- Attributes

Locations

The location tier views the grid as being made up of geographically separate facilities or groups of nodes. The HP Medical Archive can be deployed as a Single Site (Site A) or Single Site + DR (Site A and Site B).

Nodes

Within the context of the HP Medical Archive system, a node is a server hosting a collection of one or more grid services. Physically, a server is a computer with associated storage and network resources. Logically, a node hosts services that the NMS can monitor and manage. (The NMS itself is a service that runs on one or more servers.)

Services

A service is a software module providing a set of capabilities to the HP Medical Archive system. They are discussed in detail in Chapter 5.

Each service consists of components that deliver a particular capability. Each node of the grid has a predefined set of services that it hosts.

Services are typically identified by a three letter acronym.

Components

A component within a service delivers a particular capability. Each component has a set of configurable attributes that can be monitored automatically.

Services contain one or more components. Each component contains a set of attributes.

Components have names defined by the software.

Attributes

The most granular level of the system is an attribute. This is a single value or property of a component in a service. Attributes are the elements that are monitored for alarm states and may be included in reports.

Every component contains a set of attributes associated with the capability it enables.

Capabilities

For each service and component the NMS interface presents four tabs, one for each capability:

- Overview—property information about the service or component. You can use this capability to trace alarms, generate immediate reports (page 39), and get an overall sense of a service or component's performance.
- Alarms—showing the status of monitored attributes and reporting alarm histories, enabling you to trace and troubleshoot current alarms and analyze alarm histories to prevent future problems.
- Reports—for generating reports on current and historical conditions of attributes to monitor and improve system performance.

- Configuration—to set or change service settings or alarm monitoring conditions.

Consult the specific service descriptions in Chapter 5 for details of the exact information and Chapter 6 for settings available.

Software Requirements

Accessing the NMS requires access to a web browser with grid access to a well-known address (defined by your system administrator).

At this time, the only supported browser is:

- Microsoft **Internet Explorer** v6.0 SP2 (and above)
  - JavaScript and cookies must be enabled

To view the customized and dynamic graphics used by the NMS, you must also download and install:

- **Adobe SVG Viewer** plug-in

  The plug-in is available from the Adobe web site: www.adobe.com/svg/viewer/install/

This viewer supports Scalable Vector Graphic technology (SVG); a powerful tool used for high quality graphics that are dynamically created from real-time data.

Accessing the NMS

The Network Management System (NMS) can be accessed using a supported web browser (page 5).

Both the user name and password are case sensitive.

You require a user name and password to access the system. Each system user is assigned their user name and password when first introduced to the NMS. If you did not receive a user name and password, contact your system administrator. (See "Managing User Accounts" on page 7 for more information.)

Log in

Once you have accessed the NMS via your browser, the HP Medical Archive log in... window appears.

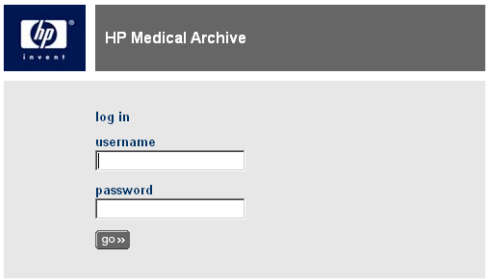


Figure 1: NMS log in Window

To log into the NMS:

1. Click in the username field to place the cursor in the field.
2. Type your username (case sensitive).
3. Press **<Tab>** to move the cursor to the password field.
4. Type your password (case sensitive). Keystrokes appear as asterisks (*) to protect your password.
5. Click the **GO** go » button to access the NMS interface.

   Your grid map appears. See the next chapter for information on using the interface.

If the username or password you entered could not be validated, the window shows an appropriate message in red (such as "Invalid user name. Please enter a valid user name and password.") below the password field. Repeat the login process to correct your entry.

If you have forgotten your password, contact HP technical support to have your password reset.

Log Out

When you have finished your NMS session, be sure to log out to keep the system secure. The **Logout** arrow Logout button is located under the System Status icon at the top right corner of the screen.

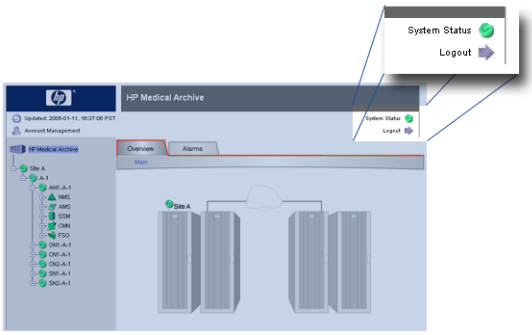


Figure 2: Location of the Logout Button

To log out:

1. Click on the **Logout** arrow button to log out.

   The Network Management System log in... screen appears with the message "Logged out" displayed below the password field.

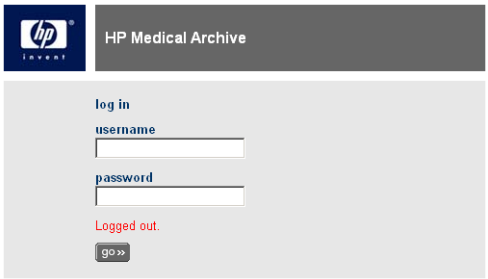


Figure 3: Successful Log Out Window

2. You may safely close the browser or continue using other applications.

Failure to log out may permit other (unauthorized) users of the workstation to continue accessing your NMS session. Note that simply closing your browser is *not* sufficient to log out of the session.

Managing User Accounts

At the time of installation, default user and group accounts are configured for you. There is an account for system technical support (Vendor) that has full permissions. The account for your use is the Admin user. These accounts cannot be deleted.

You may only alter the Password, First Name, and Last Name for your account.

To access the account management panel of the NMS:

1. Click on the **Account Management** button in the top left of the Header frame (Figure 2 on page 7).

   The Account Management tab appears in the Content frame. Using the Admin account, only your own account and group appear.

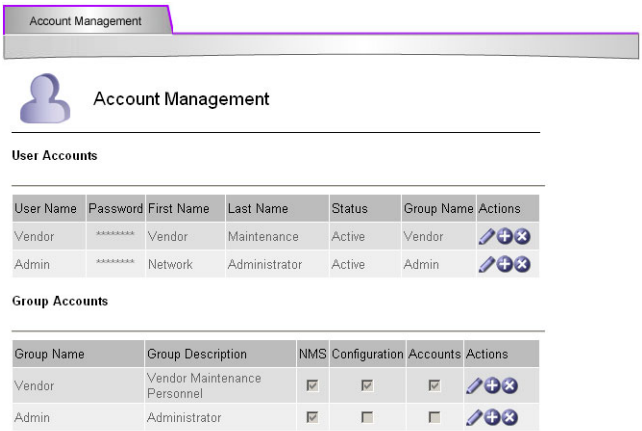


Figure 4: Sample Account Management Tab

To return to the usual NMS content tabs, select any item in the Navigation tree.

Account Management Configuration

User accounts are configured to use a group account profile to control permissions within the NMS. Action buttons are used to make changes to account settings.

Table 1: Account Configuration Controls

Action	Description
	Edit the settings for the row. This enables the fields in the row to be edited. It also enables the Apply button at the bottom of the page. Changes are not committed until the Apply button is selected. The default HP Medical Archive accounts and groups cannot be deleted. Only the password, first, and last name can be edited.

Table 1: Account Configuration Controls (cont.)

Action	Description
	Disabled for the Admin account.
	Disabled for the HP Medical Archive default accounts.

The accounts and groups displayed indicate the profile of an account and the permissions that each profile supports.

Table 2: Account Management Attributes

Attribute	Type / Units	Description
User Accounts		
User Name	Text	The user name entered at login.
Password	Encrypted	Masked password for the account; shown as a string of asterisks.
First Name	Text	User's first name.
Last Name	Text	User's last name.
Status	Enumerated text	The current status of the account: Active—the user can log in and use NMS Disabled—the user account is prevented from logging in.
Group Name	Text	Case sensitive reference to an entry defined in the Group Accounts table. The profile governs the permitted activities for user accounts within this group.
Group Accounts		
Group Name	Text	A case sensitive user defined profile name. This name is referenced in the Group Name for a user account.
Group Description	Text	User-defined description; the intent of the user group profile.
NMS	Check box	Enables access to monitor the grid using the NMS. This excludes access to some Configuration tab items.
Configuration	Check box	Enables access to the Configuration tab Main page of the CMN service.

Table 2: Account Management Attributes (cont.)

Attribute	Type / Units	Description
Accounts	Check box	Enables full access to the Account Management tab. When deselected, the user can access the tab to: • View only their own account settings • Edit their password, first and last name

Editing Your Account

All users can access the settings for their own account. The action buttons for inserting a blank line and deleting a line are disabled. You can edit your entry to change the password, first, and last name.

You may need to configure your browser to permit popups from this site.

1. Click the edit button on the line in the User Account table to enable entry fields.
2. To change your password:
   a. Double-click the Password entry to select the complete field.
   b. Type a new password and press **<Tab>**. A popup window appears to confirm the password:

Figure 5: Password Confirmation Popup

   c. Re-enter the password in the popup window.
   d. Click the **Apply** button in the popup window to confirm the password and close the popup. If the password fails to match, a dialog appears advising you to re-enter the password (step 2a).
3. To change your real name: edit the First Name and Last Name fields.
4. Click the **Apply** button to commit the changes.

Interface Components

2

Navigating the NMS Interface

Chapter Contents

Frames 12

Header 12
- Refresh Time 13
- System Status Indicator 14
- Logout Button 14
- Version Information 14

Navigation Tree 15
- Tree Structure 15
- Status Indicators 16

Content Frames 16
- Tabs 16
- Property Information (Overview) 17
- Alarms 19
- Reports 19
- Configuration 19

Navigating Locations and Nodes 21
- Location and Node Maps 21

Frames

The NMS interface is divided into three key sections or frames:

- Header
- Navigation Tree
- Content Frame

Every "page" of the NMS interface contains these three frames.

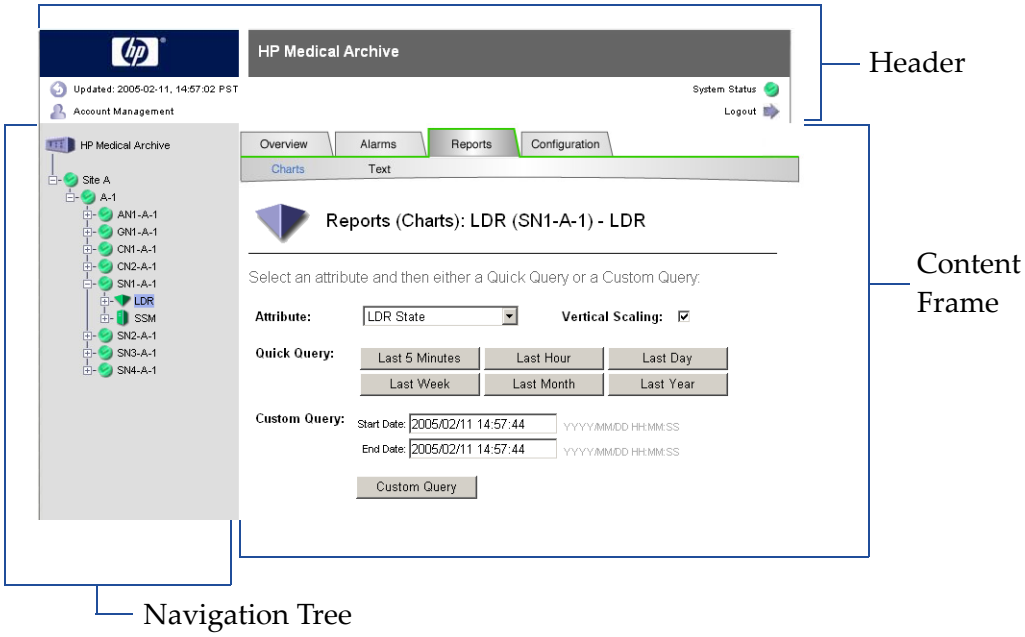


Figure 6: NMS Interface—Frames

Header

The Header frame of the NMS interface contains high-level grid status information. This frame is primarily used as a reference, providing a quick overview of the grid's vital statistics as well as buttons to manage user accounts and log off of the NMS system.

The latest refresh date and time are shown on the far left along with the Account Management button. The right side contains the System Status icon and the Logout button. The Hewlett-Packard logo in the

top left serves as a button to access the HP Medical Archive Management Interface version information.

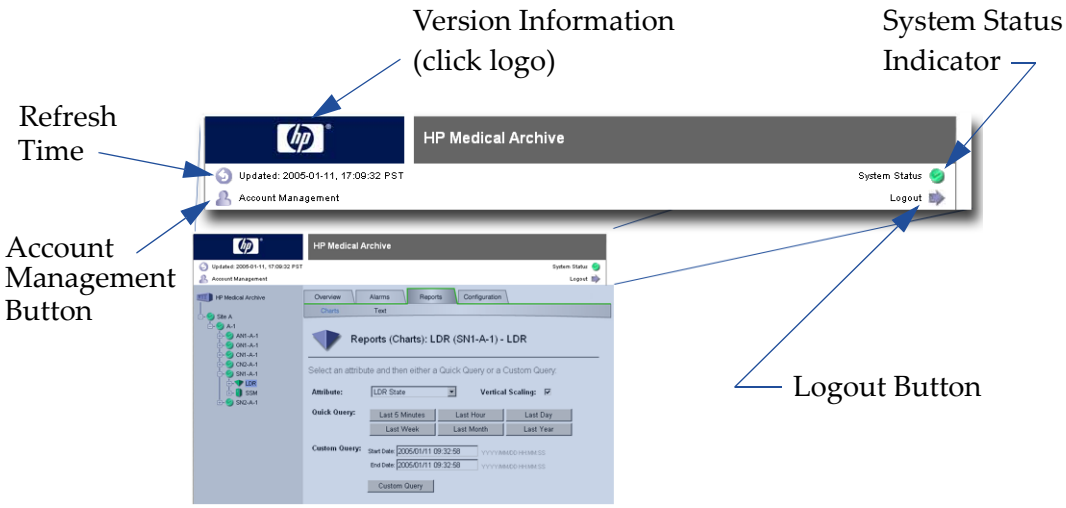


Figure 7: NMS Interface—Header Frame

Refresh Time

Information presented in the NMS interface is time-sensitive. Since the interface is delivered as HTML "pages", the content shown is static. The "Updated" date and time indicates when the data shown was collected; the time at which the grid status "snapshot" was taken. The refresh information is very useful when addressing an alarm situation.

Refreshing the Display

To take a new "snapshot" of the grid status:

- Select the update icon or the date and time text

  —or—

- Select the "refresh" button on your browser (for Microsoft Internet Explorer, press **<F5>**).

After the page has finished reloading, the content is updated and the update time reflects the time you took the snapshot.

The interface automatically triggers a refresh at intervals of about one minute. Configuration pages that allow input do *not* automatically refresh, allowing you to complete your data entry without interruption.

System Status Indicator

The System Status icon indicates the highest level of alarm within the grid. If there are no alarms in the system, the icon displays a normal status (green) as seen in Figure 7 on page 13.

Select the icon to see the Grid Map ▶ Alarms ▶ Main page listing all current alarm states that are not "normal".

See "Alarm Levels and Indicators" on page 28 for a description of the range of alarm indicators. Chapter 3 covers alarms in detail.

Account Management Button

The Account Management Account Management button is used to access the Account Management tab allowing you to access user account settings. The Admin user can view their own account settings and make changes to their password and the settings for their first and last names.

Only the Vendor maintenance user has Account permission to:

- View all accounts
- Reset forgotten passwords

See "Managing User Accounts" on page 7 for more details.

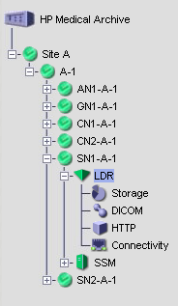
Logout Button

The Logout arrow Logout button is used to log off of the NMS, ending your session. Be sure to log off the system every time you finish a session to protect the grid from unauthorized access. See "Log Out" on page 6 for more specific information.

Version Information

Clicking on the HP logo at the top left corner of the Header frame opens a dialog with the interface version number, the software build date, and copyright information. See "Currency" on page ix for an example.

Navigation Tree



The Navigation Tree on the left side of the NMS interface displays a tree structure of the grid: the sites, cabinets, nodes, services, and components. This frame provides quick access to any element of the grid.

Naming Conventions

The names that appear in the Navigation Tree follow the following convention:

- Locations:
  - Site A—The primary site for the HP Medical Archive.
  - Site B—An optional Disaster Recovery (DR) site.
- Cabinets:
  - A-1 through A-8—Cabinets at the primary site. (Limited to A-4 if the optional DR site exists.)
  - B-1 through B-4—Cabinets at an optional DR site.
- Nodes—Named using the following elements:
  - Two or three-letter code for the type of node (such as: AN for Admin Node, GN for Gateway Node, or CSN for Control/Storage Node)
  - A sequence number (1 through 4) within the cabinet
  - The cabinet identifier (such as B-1, A-3, and so on)

    Example: GN1-A-1 is the primary Gateway Node in cabinet A-1.
- Services—Named by the software with a three letter acronym and then the node ID in parenthesis, such as ADC (11010115) for an Administrative Domain Controller service.
- Components—Named by the software

Tree Structure

By clicking on the +/- sign to the left of a name, you reveal/hide the list of related grid elements on that branch. This enables progressive disclosure of grid elements while keeping the number of items listed more manageable.

To view detailed information about an element of the grid, click on the element's name. The information is displayed in the Content frame of the NMS interface.

Status Indicators

The icon beside each location, cabinet, node, and service reflects the overall status of that part of the grid. (Components do not include a status indicator; they retain their normal icon and color.) If there are no alarms, the icon appears in the normal (green) state. If there is an alarm, the icon reflects the most severe alarm currently active on that branch of the tree (see Table 3 on page 29).

Content Frames

After using the Navigation Tree to select a grid element, you can use the Content frame to view and report on the component's status, alarms, and configuration.

Tabs

The Content frame of the NMS interface displays information on tabs appropriate to the element:

- Overview
- Alarms
- Reports
- Configuration

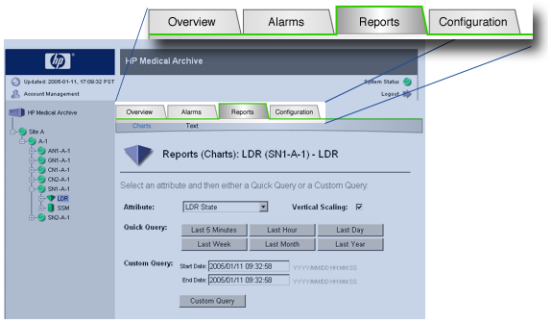


Figure 8: NMS Interface—Tabs

Some tabs do not apply to some elements. Only applicable tabs appear. Select the tab to view its contents.

Page Selectors

Some tabs organize information into “pages”. If so, a page selector appears below the selected tab. Select the page name to access that view.

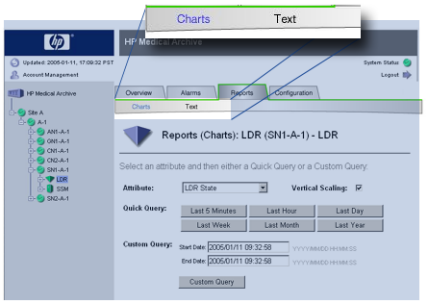


Figure 9: NMS Interface—Page Selectors

The currently selected page is shown in blue, alternate page options are in black.

Property Information (Overview)

The Overview tab provides a list of service and component attributes with their values and (if notification is active) their current status. It includes attribute information specific to the service or component; consult the specific service descriptions in Chapter 5 for details of the exact information available.

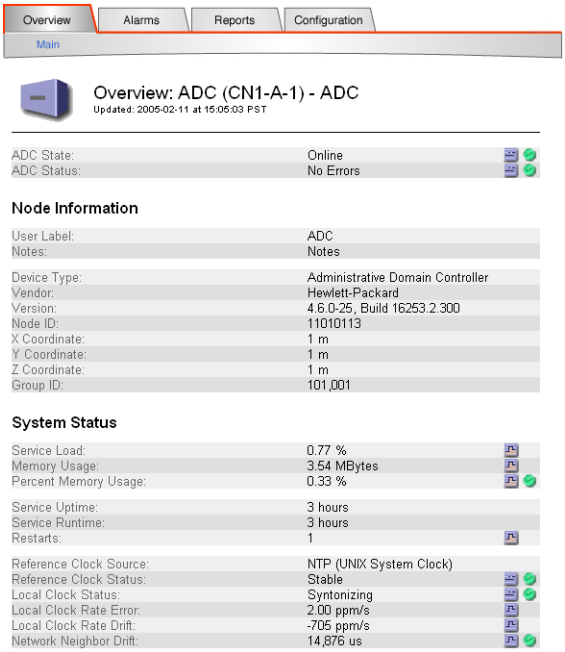


Figure 10: Sample Overview Page

Text Color

The display of attribute values normally appears black, indicating the service is running normally (reporting to the NMS). If the text appears blue, the service is in an unknown state (not reporting to the NMS) and the attribute values shown are the last known values. In cases where a service is gracefully removed from the grid (offline) the last known attribute values appear in *gray italics*.

Immediate Reports

Beside attributes that support chart style reports (“Charts” on page 42) there is an icon indicating the format of the chart available. Selecting the icon delivers the page with the Immediate report (“Immediate Reports” on page 39) for that attribute over the past hour.

Active Alarms

If an alarm status icon (Table 3 on page 29) appears beside the attribute’s name on the Overview page, alarm monitoring for that attribute is active (see “Enabling (or Disabling) an Alarm” on page 157). The attribute status can be viewed in more detail on the Alarms tab by clicking the icon.

Alarms

The Alarms tab provides information to trace the source of an alarm and to review an alarm's history. This tab offers two pages of information.

- The Main page displays a table of the attributes actively being monitored, showing their current state. Each row represents a monitored attribute and the color represents the alarm state. The table includes the attribute code, the description, and the alarm time of faults.
- The History page provides query functionality for attribute alarm histories. Reviewing the alarm history is useful for preventing grid issues and for proactive grid maintenance. The query mechanism operates in the same fashion as custom reports (page 41).

See Chapter 3 for a full description of the alarm capability.

Reports

The Reports tab starts with a form to create a quick report or custom query about a selected attribute. There are two kinds of reports available, chart and text, selected using the appropriate page option.

- The Chart page produces graphical data for the selected attribute.
- The Text page produces tables of data.

Both are useful tools for analyzing the system and for troubleshooting alarms. See Chapter 4 for a full description.

Configuration

The Configuration tab offers two pages for configuring the main properties of the service or component, and for setting the alarm monitoring features.

Some configuration items are not accessible to the Admin *account. These can only be changed using the* Vendor *account.*

- The Main page form allows you to change the state, label, and notes related to an attribute.

WARNING

Changing configuration settings requires careful and deliberate planning. Some configurable elements can affect the state of your live system. Only experienced administrators should alter the device and component configuration settings.

CAUTION

Changes to the configuration are rarely needed, and should only be undertaken after consultation with HP technical support.

- The Notification page is used to change the notification details for an attribute, as well as activating and deactivating alarms. This page gives you the ability to customize alarm settings to your specific grid needs.

CAUTION

Alarm settings are enabled as part of your installation. Changes to alarm settings should not be made for simple convenience; this may conceal underlying problems that should be resolved. If you find an alarm is persistent, discuss the situation with HP technical support before making changes.

Configuration of alarm notifications is discussed in "Alarm Configuration" on page 153 and changes to the main configuration of services and components is discussed in Chapter 6 for each service.

Navigating Locations and Nodes

Once you have logged on to the NMS, the first displayed content is a Scalable Vector Graphic (SVG) indicating two sites. Icons indicate the actual installation of Site A and Site B. As you navigate to a site, the map shows a set of cabinets (the possible maximum of eight); again, icons above the cabinets indicate the actual installation of your grid. At the cabinet level, a fully installed cabinet is schematically illustrated with icons beside the nodes actually installed. For a given node, a schematic image appears with icons for each service installed. Samples are shown in the following subsections.

Location and Node Maps

The grid's geographic locations (the primary site and optional DR site) are illustrated on the map with a status icon representing actual installation. The color of the icon gives you an immediate indication of the location's alarm state.

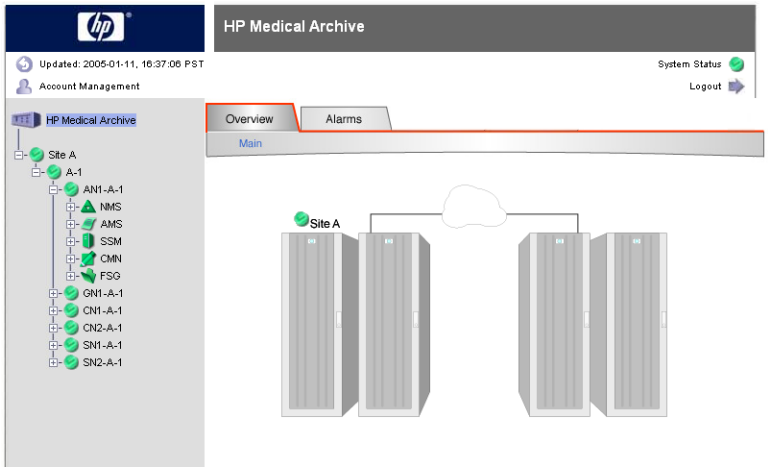


Figure 11: NMS Interface—Sample Grid Map of Locations

Clicking on an icon displays the next level (the individual location).

At this level, there are eight cabinets illustrated, the maximum possible in a single site deployment of the HP Medical Archive. (If a DR site is used, the maximum at either site is four cabinets, however the illustration shows the maximum of eight.) Only installed cabinets have an icon above them.

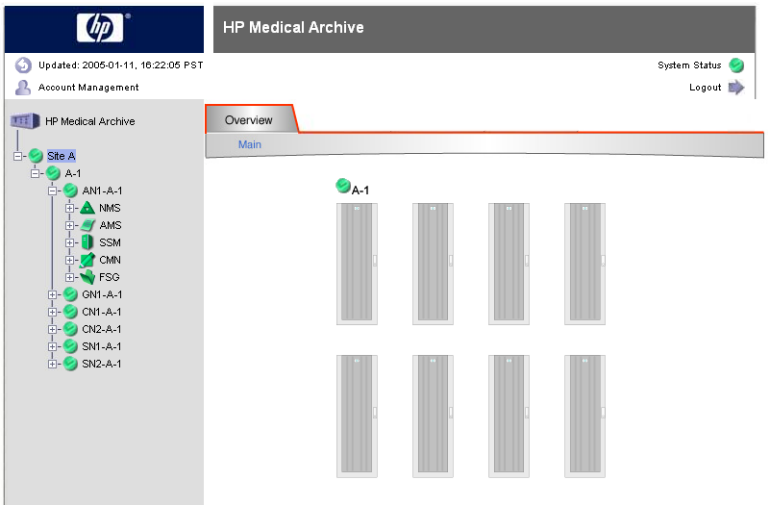


Figure 12: NMS Interface—Sample Site Map of Cabinets

Selecting a cabinet displays the map with node icons positioned where the hardware is physically located in a fully populated cabinet. The node icons appear beside the nodes that are installed in your grid. The icon reflects the alarm status of each node. The names are defined by the software as described in "Naming Conventions" on page 15.

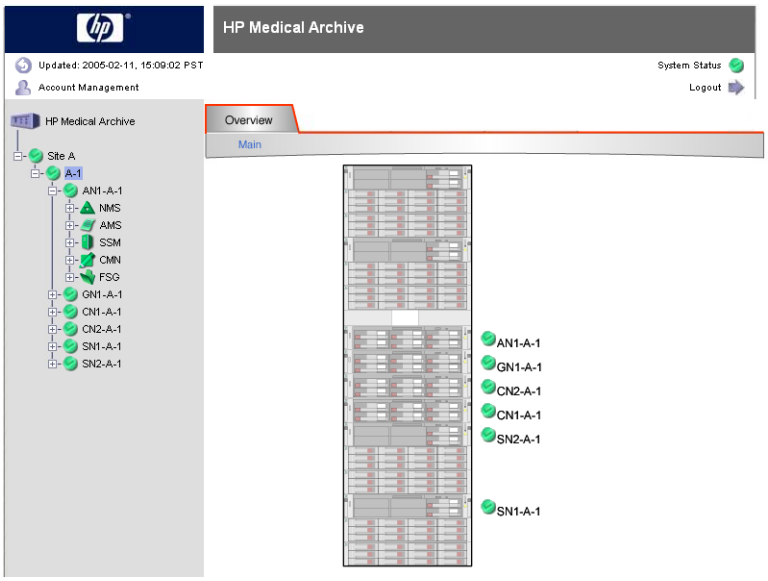


Figure 13: NMS Interface—Sample Location Map of Nodes

Every grid node typically has multiple services that are individually monitored. Clicking on the node's name displays a generic SVG map of a server with icons for the services it hosts. Each service has its own status icon appropriately colored to represent its alarm status.

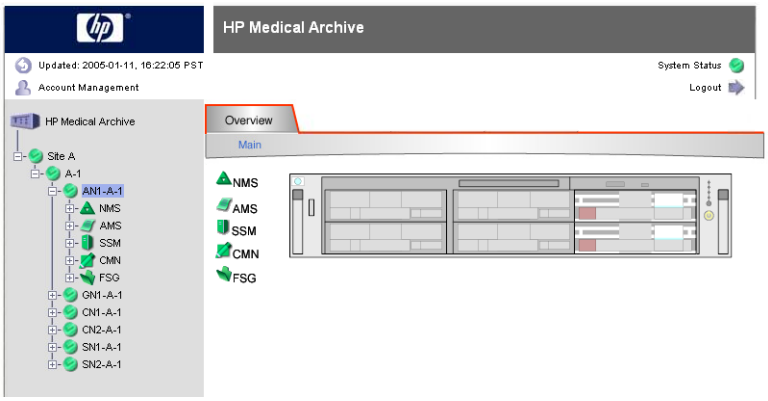


Figure 14: NMS Interface—Sample Server Map of Services

As with locations, cabinets, and nodes, you can select a service to reveal status information in the Content frame. The service/component content is more detailed. The grid map, locations, and grid nodes content displays only the Overview tab with its illustrative map. The Content frame for services and components displays the four tabs: Overview, Alarms, Reports, and Configuration discussed in "Tabs" on page 16. Click a tab to display the related content and selection forms.

Alarms

3

System Status and Notifications

Chapter Contents

System Status Overview 26
System Monitoring 26
Notifications 27
Indicators and Propagation 28

Alarm Levels and Indicators 28

Alarms Tab 30
Main Page 31
History Page 32

Alarm Handling 34
Tracing the Source of an Alarm 34
Resolving Alarms 35

System Status Overview

The Network Management System provides useful day-to-day information on the status of your grid. When a component of your grid is not performing within expectations however, the NMS becomes a critical assessment tool. Alarm indicators draw immediate attention to grid issues.

The NMS uses color-coding and icons for easy identification of alarm locations and levels. When you first view the NMS interface, the System Status icon (in the upper right corner of the page) indicates the highest alarm level on the system. You can then use the NMS tree or maps to locate the specific grid problem, assess the cause, and take quick action toward a resolution.

System Monitoring

A primary role of the NMS is to monitor grid activity and issue alarms if any attributes reach or exceed user-defined thresholds. When a tested alarm level evaluates true, that level is set.

There are six levels of alarm for each attribute; each uniquely identified (by an ID number) and individually configured. As new services are added to the grid, new alarm attribute IDs are created for it, ensuring that each alarm is uniquely associated with a specific service or component attribute and alarm level.

Unknown	187	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		
Normal	188	☑	AMQS	1	Message Queue	Normal	GE	0	UI64		
Warning	189	☑	AMQS	1	Message Queue	Over 10,000	GE	10000	UI64		
Minor	190	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		
Major	191	☑	AMQS	1	Message Queue	Over 50,000	GE	50000	UI64		
Critical	192	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		

Each monitored attribute of each service and component is tested against the configured thresholds using the algorithm shown in Figure 15.

The attribute value is tested against each enabled setting starting from the most critical and working toward normal. The “Unknown” setting is the last one tested.

When an alarm condition is found to be true, that level is checked against the current alarm level for the attribute. If there is no change, then no further action is taken.

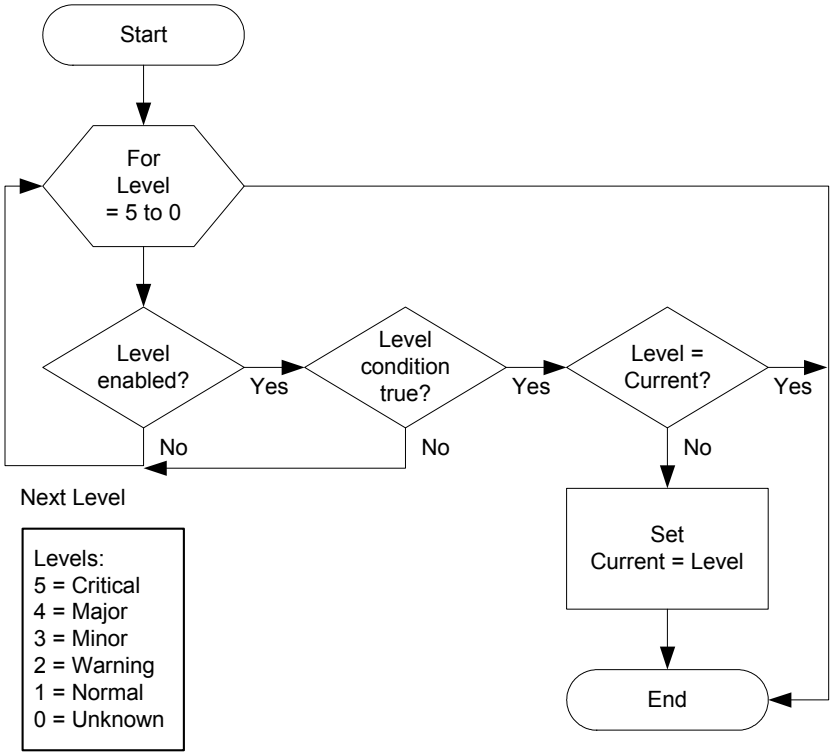


Figure 15: Alarm Monitoring Algorithm

Only if a new alarm level is detected is there a change in the alarm level reported. This automatically clears alarms when conditions return to the “Normal” level.

If an alarm level changes, the current alarm level is set and propagated up the network hierarchy as needed.

Notifications

All alarms provide indicators for informational purposes that you can check on a routine basis. The NMS is pre-configured with a default set of alarms and notification settings. You can easily customize these settings to reflect your company’s network monitoring methodology.

For information on how to customize the alarm notification settings, see “Alarm Configuration” on page 153.

CAUTION

Alarm settings are enabled as part of your installation. Changes to alarm settings should not be made for simple convenience; this may conceal underlying problems that should be resolved. If you find an alarm is persistent, discuss the situation with HP technical support before making changes.

Indicators and Propagation

Alarms are generated at the attribute level of the grid. When an issue is detected, the alarm is propagated up through the grid hierarchy. The associated attribute, component, service, and node information on the NMS are all changed to reflect the alarm state. As a result, you can view the general alarm state at the grid level, then drill down through the service components to locate the specific details. (See Figure 16: “Sample Alarm Indicator Propagation” on page 30.)

Each individual service reflects the highest alarm state of its components. If more than one alarm exists on a node, the node always reflects the highest and most serious alarm level (see “Alarm Levels and Indicators” below). Locations (Site A and Site B) display the highest alarm level of the nodes on that branch.

Refer to Figure 16 on page 30 for an example. One node’s SSM indicates a minor alarm state while its LDR indicates an unknown state. That node icon displays the unknown alarm state (the higher alarm level). Another node in the same group shows a major alarm on the AMS service. The group location propagates the “unknown” alarm indicator. The color and icon of each service, node, and location reflects its highest alarm state along its branch of the Navigation Tree.

Alarm Levels and Indicators

NMS alarms are organized into a hierarchy of levels. The hierarchy reflects the seriousness of a grid issue. There are six alarm levels in the

NMS interface. Each alarm level has an associated color and icon. The NMS alarms levels (from lowest to highest) are:

Table 3: Alarm Levels and Indicators

Icon	Color	Level	Meaning
	Green	Normal	All functions are working normally.
	Yellow	Warning	An unusual condition exists that does not affect normal operation; most likely related to a component being in a standby state.
	Light Orange	Minor Alert	An abnormal condition exists that could affect operation in the future; should be investigated to prevent escalation.
	Dark Orange	Major Alert	An abnormal condition exists that is currently affecting operation; requires prompt attention to prevent escalation.
	Red	Critical	A critical alert of an abnormal condition that has stopped normal operation; should be addressed immediately.
	Blue	Unknown / Offline	An unknown condition exists that has stopped normal operation. Requires immediate attention.

The "Unknown" alarm level is considered very severe if it is enabled and detected, although it is the last level tested in the alarm monitoring algorithm (Figure 15 on page 27). Most attributes do not enable this level.

Each alarm level has its own icon and color. These icons and colors are used throughout the NMS interface to save you time when analyzing a critical grid situation. Alarm colors and icons accelerate alarm identification and resolution by making the alarm source quickly visible on the NMS interface. The System Status icon in the Header frame immediately indicates the most serious alarm level of the grid. The icons on the Network Map indicate the status of each location or node. You can then follow the tree branch to the individual service to find the source of the alarm.

Nodes display the alarm icon of the highest alarm state among their hosted services (Figure 16). Note that each service *retains* its unique icon, but the *color* changes to reflect its current alarm state. Component icons and colors, however, remain unchanged regardless of the alarm state.

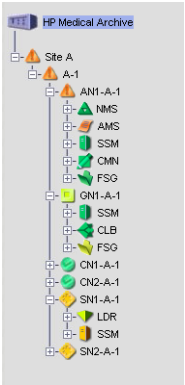
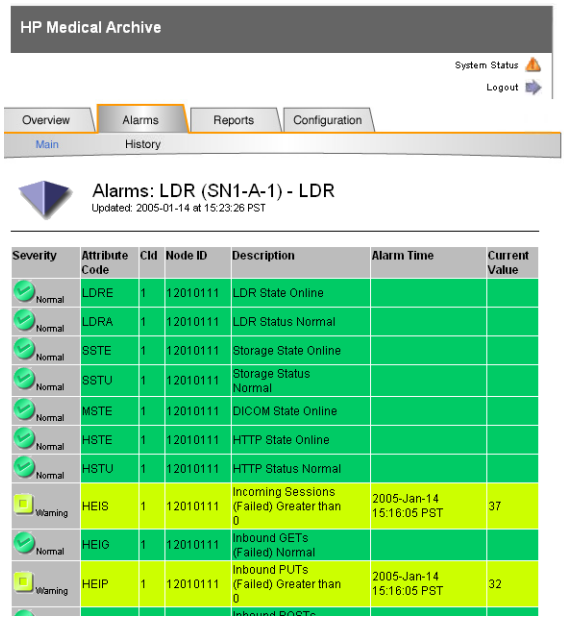


Figure 16: Sample Alarm Indicator Propagation

Alarms Tab

Under the Alarms tab of each service or component, colors highlight critical alarm information (Figure 17). By default, the table rows are green to indicate a normal status. If the status of an attribute changes, an alarm row for that attribute changes to the appropriate color (Table 3 on page 29).



Severity	Attribute Code	Cld	Node ID	Description	Alarm Time	Current Value
Normal	LDRE	1	12010111	LDR State Online		
Normal	LDRA	1	12010111	LDR Status Normal		
Normal	SSTE	1	12010111	Storage State Online		
Normal	SSTU	1	12010111	Storage Status Normal		
Normal	MSTE	1	12010111	DICOM State Online		
Normal	HSTE	1	12010111	HTTP State Online		
Normal	HSTU	1	12010111	HTTP Status Normal		
Warning	HEIS	1	12010111	Incoming Sessions (Failed) Greater than 0	2005-Jan-14 15:16:05 PST	37
Normal	HEIG	1	12010111	Inbound GETs (Failed) Normal		
Warning	HEIP	1	12010111	Inbound PUTs (Failed) Greater than 0	2005-Jan-14 15:16:05 PST	32

Figure 17: Sample Alarms Tab

Each row provides detailed information about the alarm (see Table 4 on page 31 for details). More detailed information about each attribute's code, value, and definition can be found in Chapter 7, "Troubleshooting Alarms" on page 171.

Once the alarm is resolved, the alarm returns to the green status to indicate that the attribute has returned to a normal state.

You can access and view alarm status at both the service and the component levels. There are two pages under the Alarms tab: Main and History. When the tab is selected, it defaults to the Main page, which provides details of the current status.

Main Page

The Main page of the Alarms tab gives the current status of the selected service or component attributes. This page is an overview of each attribute's current alarm level. You can use this page to get a quick, but detailed, sense of what may be causing a system alarm. The Main page can also be used to track the daily status of the system in order to prevent major alarms.

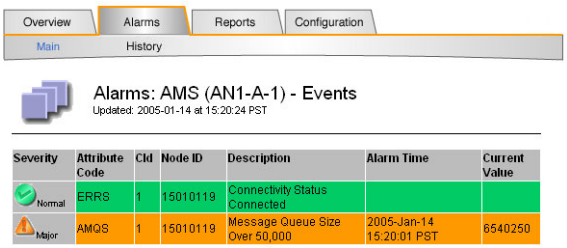


Figure 18: Sample Component Alarms Tab—Main Page

The alarm data is listed in a table with the following headings:

Table 4: Alarm Table Headings

Heading	Definition
Severity	Color icon indicating alarm level (see Table 3 on page 29)
Attribute Code	Code that identifies the attribute and issue being monitored (see Chapter 7 for an alphabetical lookup table)

Table 4: Alarm Table Headings (cont.)

Heading	Definition
CId	"Cell ID", a secondary identifier used when a monitored attribute is a cell in a table, such as the Status attribute of the SSM ▶ Volumes component (VMST). The CId indicates the corresponding row in the attribute table.
Node ID	Unique number identifying the service within the grid. This number is assigned at installation.
Description	Brief details about the cause of the alarm; consisting of the Primary Message and Secondary Message in the alarm configuration.
Alarm Time	Date and time stamp of the last attribute report from the service or component.
Current Value	Value of the attribute as last reported by the service or component.

History Page

The History page enables you to perform queries on the history of an attribute. Alarm history provides perspective on whether an attribute has been triggering frequent alarms. These statistics allow you to address deeper grid issues and prevent future alarms.

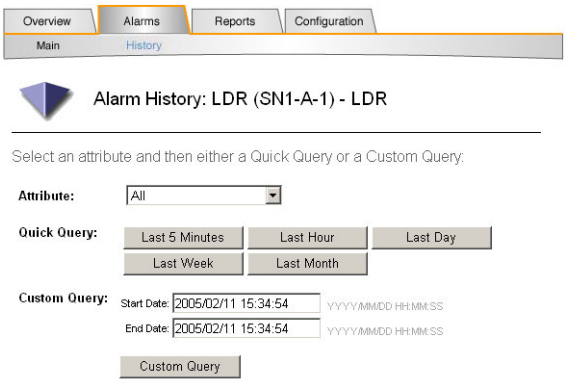
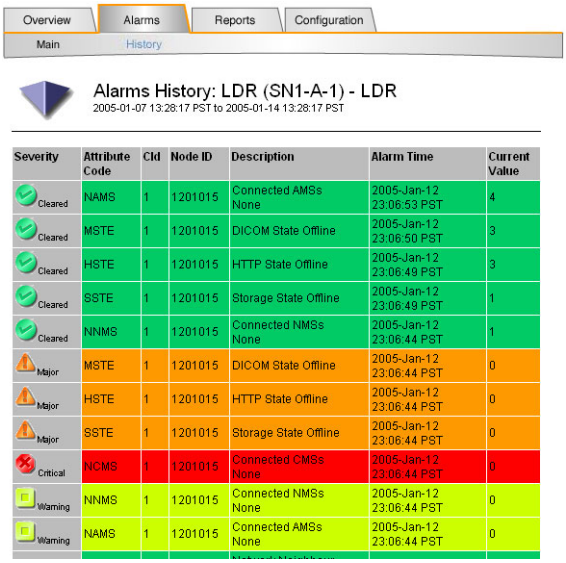


Figure 19: Sample Alarm History Request Form

You can perform a quick or a custom query (the same selection mechanism as standard reports). Quick queries generate results for a predefined time range with the click of a single button. Custom

queries provide data based on your specified time and date requirements. For more information on performing queries, see page 39.

The generated data displays in a table with the same headings shown on the Main page (see Table 4 on page 31). This data is listed sequentially based on the time of an alarm's change in state. The most recent change is listed first.



Severity	Attribute Code	Cid	Node ID	Description	Alarm Time	Current Value
Cleared	NAMS	1	1201015	Connected AMSs None	2005-Jan-12 23:06:53 PST	4
Cleared	MSTE	1	1201015	DICOM State Offline	2005-Jan-12 23:06:50 PST	3
Cleared	HSTE	1	1201015	HTTP State Offline	2005-Jan-12 23:06:49 PST	3
Cleared	SSTE	1	1201015	Storage State Offline	2005-Jan-12 23:06:49 PST	1
Cleared	NNMS	1	1201015	Connected NMSs None	2005-Jan-12 23:06:44 PST	1
Major	MSTE	1	1201015	DICOM State Offline	2005-Jan-12 23:06:44 PST	0
Major	HSTE	1	1201015	HTTP State Offline	2005-Jan-12 23:06:44 PST	0
Major	SSTE	1	1201015	Storage State Offline	2005-Jan-12 23:06:44 PST	0
Critical	NCMS	1	1201015	Connected CMSs None	2005-Jan-12 23:06:44 PST	0
Warning	NNMS	1	1201015	Connected NMSs None	2005-Jan-12 23:06:44 PST	0
Warning	NAMS	1	1201015	Connected AMSs None	2005-Jan-12 23:06:44 PST	0

Figure 20: Sample Alarm History Report

Rows showing the green icon show either:

- "Cleared"—an attribute has returned to "Normal" from one of the alarm states other than "Unknown".

  —or—
- "Normal"—an attribute has returned to normal state from the unknown state ( ) and the description shows "State Change Unknown to Active".

To return to the history request form from an alarm history table, click the **History** page selector.

Analyzing Alarm Histories

Queries on the alarm history page provide valuable analytical information. You can query for data about a specific attribute or for all of the alarms that have occurred on a node over a specified period of time.

These queries are a powerful grid diagnostic tool, enabling you to identify alarm patterns and service issues. Regularly reviewing alarm patterns can resolve minor issues before they impact grid functionality. At the very least, reviewing the alarm history gives an overview of how the system is functioning and may help to prevent future alarms.

Alarm Handling

The NMS is a critical tool for responding to system alarms. When you receive an alarm notification, the NMS provides the data necessary to resolve the issue. This section provides step-by-step procedures for investigating, evaluating, and responding to alarms.

Tracing the Source of an Alarm

Tracing an alarm follows these main steps (each is expanded later in the text):

1. Trace through the network tree to the specific node generating the alarm.
2. Use the information from the Alarms table to identify the component and attribute causing the alarm.
3. Troubleshoot the alarm by using the lookup table in Chapter 7, “Troubleshooting Alarms” on page 171.

1. Locate the Source of an Alarm

a. **Log in** to the NMS to display the Network Map. Use the icons and color codes (Table 3 on page 29) to determine which location has triggered the alarm.
b. Select the **Site** that is displaying the alarm icon to view the cabinet icons for that location. Use the icons and color codes to determine which cabinet has triggered the alarm.
c. Select the **cabinet** that is displaying the alarm icon to view the node icons for that cabinet.
d. Select the **node** with the alarm icon to view the service icons for that node. Use the color codes to determine which service has triggered the alarm.
e. Select the **service** with the alarm color to access the service’s Overview page.
f. Select the **Alarms ▶ Main** page to view the summary table of monitored attributes for the service and its components. Locate

the row in the table highlighted in the alarm color. Note down the following information:

- **Attribute Code**—the four-letter identifier for the alarm type
- **Description**—the message explaining the alarm

2. Identify the Component and Attribute

a. Using the Description from step **1**, determine if the alarm is associated with a specific component. Select the **component** to view its Alarms ▶ Main page to find the alarm.

b. Select the **Configuration ▶ Notification** page to view the list of monitored attributes for that service or component.

c. Find the rows with the **Attribute Code** noted in step **1**. above.

d. Determine the specific condition for the alarm from the settings in that row.

3. Troubleshoot the Alarm

a. Look up the four-character **Attribute Code** from step **1** in the "Alarm Reference Table" on page 172.

b. Follow the suggested actions for the attribute.

Resolving Alarms

Most alarm conditions are temporary situations of grid load and resolve themselves over time. Always consult Chapter 7 for troubleshooting advice. For persistent alarms, contact HP technical support after following the suggested actions.

Clearing Alarms

Alarm states are self-correcting when the attribute value for an alarm returns to normal. Once a grid issue has been resolved, the alarm details can be viewed under the Alarms ▶ History page (see page 32). You can perform queries to retrieve data for preventive analysis.

Alarms related to counted events, such as HTTP sessions failed, can often be reset using a check box on the component's Configuration ▶ Main page. See Chapter 6.

Reports

4

Current and History Reporting

Create, view, and print reports on system attributes and status alarm histories.

Chapter Contents

Introduction to Reporting 38

Accessing Reports 39
- Immediate Reports 39
- Quick Reports 40
- Custom Reports 41

Report Formats 42
- Charts 42
- Text Reports 44

Chart View Controls 45
- Window 45

Printing Charts and Reports 46

Introduction to Reporting

Reports are a powerful system analysis and troubleshooting tool. The NMS can generate reports at both the service and the component level, although some individual attributes do not have reportable events. These reports provide an overview of how a system attribute is functioning over a selected period of time. By viewing a report, you can quickly ascertain if the attribute has any issues.

Reports are also valuable to track the data flow on the grid. You can view how much data enters the grid each day, how many audit messages are being sent, and whether the data storage capacity is sufficient. You always know the state of resources on your grid.

The NMS provides a variety of report query options and displays. You generate reports with the simple click of a button or by requesting a custom report according to specific time spans. The generated report can be displayed in a graphical chart or a text table. You can then print the final report, or copy it for use in documents.

Report Types

The NMS provides three different ways to generate reports:

- Immediate—generated by the click of a button on the Overview page.
- Quick—created through preset criteria selections on the Reports page.
- Custom—a form on the Reports page enables you to specify your requirements, providing feedback specifically customized to your needs.

Charts and Text Reports

Reports take one of two forms: chart or text. Charts present the data in a graphical view. Text reports are a simple text table with row entries for each event that an attribute reported. Both types are described in greater detail later in this chapter.

The format is determined by the page from which you select the report. Immediate reports are always charts, selected from the Overview page. Quick and Custom reports are available from both the Reports ▶ Chart and Reports ▶ Text pages.

Accessing Reports

Reports are accessed in one of two ways:

- Immediate reports are accessed by clicking the chart icon on the Overview tab for the service or component.
- Quick and Customized reports are accessed from a form on the Reports tab under either the Chart page or the Text page.

Under the Reports tab, each service and component has select attributes for which reports can be generated. Individual service details in Chapter 5 indicate whether attributes are reportable. In some cases, the attributes available under the chart and the text pages differ.

Immediate Reports

Immediate reports are available on the Overview page for reportable attributes, indicated by a chart button at the right side of the page.

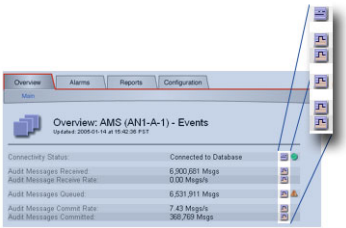


Figure 21: Sample Immediate Report Buttons

The button graphic reflects the type of graph that is presented. The graph style is preconfigured to best present the attribute's data.

Table 5: Immediate Report Buttons

Button	Report Type	Presentation
	Level	Bar graph
	Bar	Bar graph
	State	Line graph

When a button is selected, a chart report is generated and the NMS view changes to the Reports tab.

To generate an immediate report:

1. Navigate to the service or component you want to report on. The item's Overview page appears.
2. Scroll to the attribute you want to chart. If reports can be generated for the attribute, the appropriate report button is available at the far right of the attribute's row.
3. Click on the report button. The Reports page appears and the requested chart is displayed.

The report displays the attribute's data over the past hour, a preset time span. To view other time ranges, or to see a wider (zoom out) or narrow (zoom in) range of time use either the Quick Reports or the custom report form.

Quick Reports

Quick reports are available on the Reports tab, from both the Chart and Text pages.

There are six options specifying the time span for the report, ranging from the last 5 minutes to the last year. Quick reports can be generated with the selection of an attribute and then the push of a time span button.

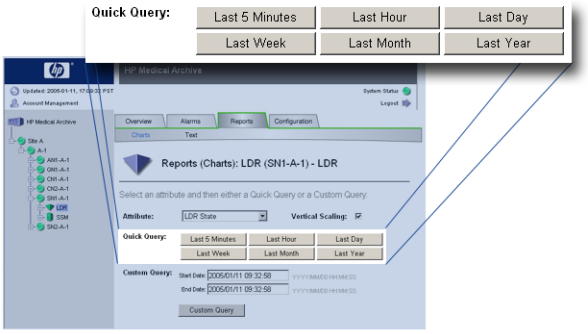


Figure 22: Report Request Form—Quick Reports

To generate a quick report:

1. Navigate to the service or component you want to report on. The item's Overview page appears.
2. Select the **Reports** tab. The Charts page appears by default.

3. Optionally deselect the **Vertical Scaling** check box to force the Y-axis to start at zero. This option is selected by default, allowing the Y-axis to cover a range that best fits the data.

   —or—

   Optionally select the **Text** page to obtain a text format report.
4. Use the **Attribute** pull-down menu to select the attribute to report.
5. Select the Quick Query button for the desired duration of the report. The report appears after a few moments.

Although the Content frame may update fairly quickly, charts can take some time to tabulate and form the image. Allow several minutes for tabulation of long time ranges.

Custom Reports

Custom reports present in the same way as quick reports but add the ability to customize the time span of the data (down to the second) to be displayed. Both Chart and Text pages support custom reports.

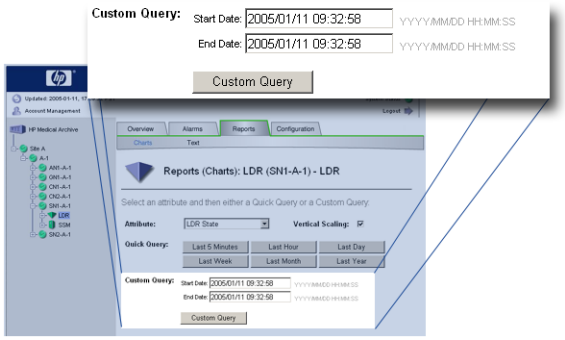


Figure 23: Report Request Form—Custom Reports

To generate a custom report:

1. Navigate to the service or component you want to report on. The item's Overview page appears.
2. Select the **Reports** tab. The Charts page appears by default.
3. Optionally deselect the **Vertical Scaling** check box to force the Y-axis to start at zero. This option is selected by default, allowing the Y-axis to cover a range that best fits the data.

   —or—

   Optionally select the **Text** page to obtain a text format report.
4. Use the **Attribute** pull-down menu to select the attribute to report.

5. In the Custom Query panel, enter the **Start Date** and **End Date** for your report. Use the format YYYY/MM/DD HH:MM:SS for both entries.
6. Select the **Custom Query** button to generate and display the report. The report appears after a few moments.

CAUTION

Allow several minutes for charts to appear. Although the Content frame may update fairly quickly, charts can take several minutes to tabulate and form the image. Do not initiate another report request until the current one has completed.

To view other time ranges, or to see a wider (zoom out) or narrow (zoom in) range of time, modify the start and end dates in the custom report form.

Report Formats

Chart and text reports present essentially the same data in very different ways. You can use each report format to suit your specific reporting needs. Chart reports give a graphical presentation of data. Text reports give the basic data in a simple table with no customization options after the report has been created.

Charts

Chart reports present the data with the attribute values (vertical axis) over a specified time span (horizontal axis). The types of chart reports available are detailed below. If the numbers in the chart represent a volume portion (such as the percentage of memory being used), the area under bars is shaded. If the numbers represent exact values (such as the number of system restarts), the bars appear as a simple line with no shading.

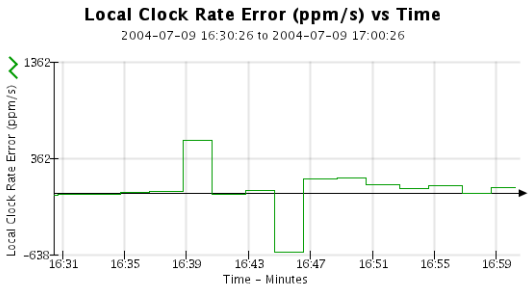
Interpreting Lines and Shading

Charts use color and shading to convey specific information about the graph.

Table 6: Chart Colors and Shading

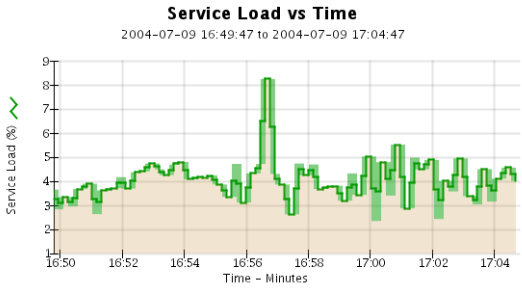
Sample	Meaning
	Reported attribute values are plotted using dark green lines.
	Light green shading around dark green lines indicates that the actual values in that time range vary and have been “binned” together for faster plotting. The range in light green indicates the maximum and minimum values within the “bin”. Light brown shading is used for bar graphs to indicate volumetric data.
	Light purple shading indicates that the attribute value at that time was indeterminate; the attribute was not reporting.
	Blank areas (white, no data plotted) indicate that the attribute was unavailable. The service or component was known to be offline, so no data exists for that time range.

Level Graph



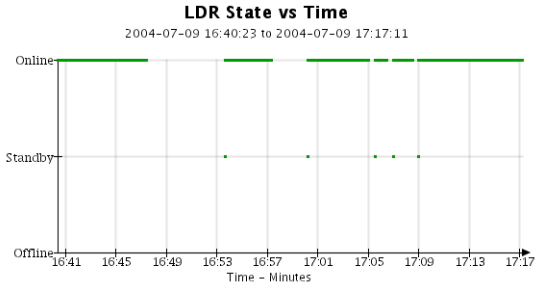
Level graphs are used to plot the values of an attribute that has a “unit” value (such as Local Clock Rate Error, in ppm). The changes in the value are plotted in “bins” at regular intervals over time.

Bar Graph



Bar (area) graphs are similar to level graphs but include a light brown shading below the line. These are used to plot the values of an attribute that has a "quantity" value (such as Service Load, a percentage). The changes in the value are plotted in "bins" at regular intervals over time.

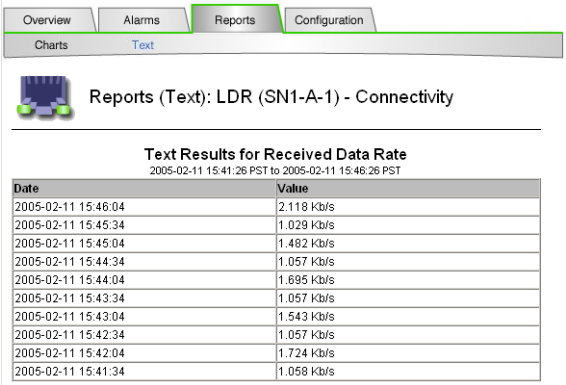
State Graph



State graphs are similar to level graphs but the transition is discontinuous; that is, the value jumps from one state (value) to another. These are used to plot values that represent distinct states (such as a service State, that can be online, standby, or offline). The changes in the value appear as distinct horizontal lines at predefined levels on the chart.

Text Reports

Text reports present the data in a simple table with the date and time in the first column and the attribute values in the second column. They give the basic data in a simple format without any of the additional overview information provided in a chart report.



Date	Value
2005-02-11 15:46:04	2.118 Kb/s
2005-02-11 15:45:34	1.029 Kb/s
2005-02-11 15:45:04	1.482 Kb/s
2005-02-11 15:44:34	1.057 Kb/s
2005-02-11 15:44:04	1.695 Kb/s
2005-02-11 15:43:34	1.057 Kb/s
2005-02-11 15:43:04	1.543 Kb/s
2005-02-11 15:42:34	1.057 Kb/s
2005-02-11 15:42:04	1.724 Kb/s
2005-02-11 15:41:34	1.058 Kb/s

Figure 24: Sample Text Report

The Date column lists the local date and time of attribute reports. The Value column displays the attribute's value for each report.

This detailed breakdown of data can result in very long tables. Text reports are therefore better suited to shorter, more specific time spans.

Text reports support some attributes—such as changes to text attributes—that are not available in chart form.

Chart View Controls

When you generate a chart report, it may be useful to compare the results with another chart. The NMS provides the ability to view the data in a new window; to hold it while using the main interface to select other reports or views.

To see other time ranges of data, use the custom report form to select the desired range. Narrowing the time span "zooms" in on the data for detailed analysis.

Window

To capture the current view for comparison with other chart views, you can place the chart in a new window (kiosk). You may open as many of these kiosk views as you wish.

Opens a new window and displays the current view.

When you are done, use your operating system's window close button to close these chart windows.

Printing Charts and Reports

Reports of any type can be printed—as can any other page of the NMS interface—by using the print function of your browser.

Using Microsoft® Internet Explorer:

1. Create the desired report (or other content page).
2. Right-click in the Content frame to access the context menu.

   Note that where you right-click determines the context menu you get. Right-clicking in the title area of the Content frame yields the menu shown at left; over the chart yields the menu on the right.

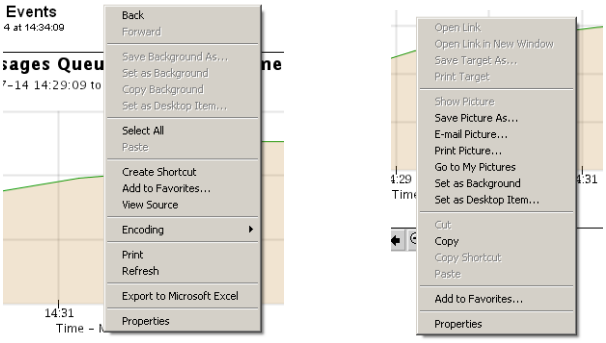


Figure 25: Browser Context Menus

3. Select either **Print** or **Print Picture...** from the context menu to open the Print dialog.
4. Use the dialog to make appropriate selections for your needs. Depending on the context menu used, the Options tab in the dialog may offer you the selection to print **Only the selected frame**. This is the recommended option. See "Print Options" below for a more detailed discussion.
5. Select **Print** to send the page to your printer.

Print Options

When printing a chart frame, there are two possible outcomes:

- Printing from the frame context menu; printing only the selected frame yields a page with:
  - Content frame heading (service, component, and icon)
  - The chart itself with its title
  - Chart window button
- Printing from the image context menu drops the Content frame heading and chart window button, yielding only the chart itself along with its title.
- Printing from a new window ( ) using the image context menu yields the Content frame heading (service, component and icon) and the chart (with its title).

Text reports print as normal web pages with: the Content frame title, the table title, and the table data.

Services and Components

5

Reference information on service and component attributes.

Chapter Contents

Overview of Services and Components 50
- Services 50
- Service Components 51
- Interpreting Attribute Description Tables 54

ADC—Administrative Domain Controller 56

AMS—Audit Management System 61

CLB—Connection Load Balancer 67

CMN—Configuration Management Node 76

CMS—Content Management System 94

FSG—File System Gateway 102

LDR—Local Distribution Router 115

NMS—Network Management System 132

SSM—Server Status Monitor 138

Overview of Services and Components

The NMS categorizes system information by the services and service components found on each node. These services and components contain attributes that form the basis for the NMS alarm notification and report options.

This chapter provides a complete list of NMS services and components. Services are listed alphabetically.

Not all grids use every service and component listed here. Each grid uses only those services and components suited to the options purchased and the functionality required.

Services

Grid services are programs that run on the physical servers (nodes). Each delivers particular services to the grid as shown in Table 7. The NMS is used to access the critical information gathered by these services so that you can monitor the condition and performance of your grid.

By clicking on the service name in the NMS, you can view detailed data about the service and each of its component functions. The NMS provides basic functional statistics, alarm status, reporting functionality, and configuration options for each service and node.

Table 7: HP Medical Archive Services

	Icon	Tag	Service Name	Function	Pg
Data Plane		LDR	Local Distribution Router	Storing and routing data through the grid.	115
		CLB	Connection Load Balancer	Enabling storage and retrieval through the DICOM protocol option.	67
		FSG	File System Gateway	Enabling storage and retrieval through standard network file systems.	102

Table 7: HP Medical Archive Services (cont.)

	Icon	Tag	Service Name	Function	Pg
Control Plane		CMS	Content Management System	Storing and managing metadata for the content.	94
		ADC	Administrative Domain Controller	Authenticating and managing IP address ranges and nodes, managing system timing, and reporting network topology.	56
Management Plane		SSM	Server Status Monitor	Monitoring server activity and hardware.	138
		NMS	Network Management System	Notifying administrators of alarm conditions and providing the user interface for grid management.	132
		CMN	Configuration Management Node	Managing system configuration through the NMS interface. Access to changing settings in this service is restricted to the Vendor account.	76
		AMS	Audit Management System	Logging grid transactions for audit and reporting.	61

Within a grid, the same service can be installed and used on more than one node. The settings made to a service on one node do *not* affect the settings on the same service installed on a different node. System-wide configurations can be made by a service technician under the Vendor account using components of the Configuration Management Node (CMN).

Service Components

Each service is composed of one or more components that manage one piece of the service's functionality. When using the NMS, you can select a service's component to view the attributes that the component manages. The NMS also provides alarm status, reporting functionality,

and configuration options for each component. Table 8 (below) lists all of the available service components.

Table 8: Service Components

Icon	Name	Parent Service	Data Provided
	Connectivity	All services except SSM	Connectivity is a component of all services. The specific attributes listed in the NMS depend on the parent service. In general, this component manages information and statistics about network data transfer rates and volumes to and from the parent service, and the connection state to other services.
	Network	SSM	Network reports on the network interfaces of the server.
	Events	AMS	Statistics on the audit messages received and committed.
		SSM	Server hardware and driver logs.
	Storage	LDR, FSG	Statistics on storage used and space available.
	DICOM	CLB, CMS	Statistics on DICOM connections and transactions.
		LDR	Connectivity settings and statistics for the DICOM interface.
		CMN	Connectivity settings for the DICOM interface to the grid.
	DICOM Advanced	CMN	Configuration settings for the DICOM connection permissions and behaviors.
	DICOM Indexes	CMN	List of the DICOM tags used by the grid for content query and management.
	Audit	CMN	Configuration of the audit messages to be logged.
	FSG Groups	CMN	Configuration of the FSG replication groups, and primary and secondary settings.

Table 8: Service Components (cont.)

Icon	Name	Parent Service	Data Provided
	Grid Options	CMN	Report of grid identification information.
	Grid Tasks	CMN	Management of grid-wide programmed maintenance tasks.
	HTTP	CLB, LDR	Connectivity settings and statistics for the HTTP interface.
		CMN	Connectivity settings for the HTTP interface to the grid.
	HTTP Advanced	CMN	Configuration settings for the HTTP connection permissions.
	IP Ranges	CMN	IP ranges of permitted remote entity connections and their locations.
	NMS Entities	CMN	Report of the grid configuration with object IDs (OIDs).
	Content	CMS	Statistics on grid content ingest, replication, and purging.
	Database	CMS	Statistics on database type and transactions.
	Synchronization	CMS	Statistics on message processing and information synchronization between CMS services.
	Replication	FSG	View FSG Replication settings and activity.
	Backup	FSG	View FSG backup settings and status.
	Client Services	FSG	Status of file sharing services.
	RAID	SSM	Status of any attached RAID hardware and drives.

Table 8: Service Components (cont.)

Icon	Name	Parent Service	Data Provided
	Services	SSM	Information on the state and resource usage of services being monitored.
	Volumes	SSM	Information on the state, mount point, and space available on storage volumes connected to the service.

The NMS interface provides you with detailed information and functionality for each service and component on your nodes. Whether you are inspecting the cause of an alarm or simply monitoring components on your grid, you can use the NMS to find information.

Interpreting Attribute Description Tables

This chapter provides attribute reference information in tables that follow a standard format. Given a (partial) sample display (Figure 26):

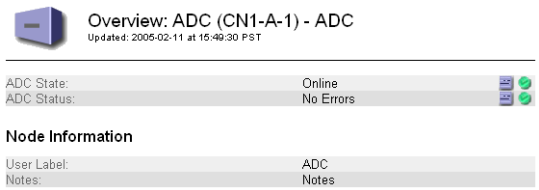


Figure 26: Partial Display Sample

The corresponding sample table (Table 9) illustrates the format. Below the sample table is an explanation of some column headings.

Table 9: Sample Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	ADCE
Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 10 = Errors	✓	✓	ADCA

Table 9: Sample Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✘	✓	N/A
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✘	✓	N/A

The Type / Units column identifies the data type or units of measure. This is useful in interpreting alarm settings and the nature of reports that can be generated. If the type is "Enumerated text", the enumerated values that the attribute can have are listed with the description of the attribute. Note that some attributes have enumerated values that can only occur under software control.

For units of "Duration" or "Bytes", the values displayed in the NMS are scaled to a suitable unit. For example, durations scale to seconds, minutes, hours, or days; bytes scale to Kilobytes, Megabytes, or Gigabytes.

The scale of bytes displayed by the NMS uses the "natural" measure of powers of 10. For example 3 MBytes = 3 x 10^6 = 3,000,000 bytes. This is not the same as powers of 2 normally used for computing, where 3 MBytes = 3 x 2^{20} = 3,145,728 bytes.

The three columns on the right indicate if the attribute can be reported in chart form (C) and text form (T), and the alarm attribute code (Alarm) used to monitor the attribute where available. In the PDF edition of this document, the alarm code is a hyperlink to the entry in Chapter 7, "Troubleshooting Alarms".

ADC—Administrative Domain Controller

The Administrative Domain Controller (ADC) authenticates the grid nodes and their connections with each other. For two nodes to connect, the ADC must have certificates for both. The ADC maintains the certificates and synchronizes this information with the other ADCs in the grid.

In general, all system nodes maintain a connection to at least one ADC. This ensures that the nodes are always accessing the latest certificates (occasionally updated or revoked). When nodes connect they cache other nodes' certificates, enabling systems to continue functioning with known nodes even when an ADC is unavailable. New nodes can only establish connections via an ADC.

The connection of each node lets the ADC gather topology information. This node information includes the CPU load, the amount of available disk space (if it has storage), the supported services, and the node's group ID (location). The grid's LDRs, CMSs, and CLBs ask the ADC for topology information through topology queries. The ADC responds to each query with the latest information received from the grid.

Group IDs are in the form of 10X00Y, where X and Y are pre-assigned based on the site and cabinet number. For example, cabinet B-3 would have a Group ID of 102003. These are used in placing replications under business rules, to permit the grid to disperse data in the most robust and efficient manner possible within the available topology.

ADC Attributes

The ADC supports the common set of service attributes. These common service attributes appear on the Overview tab for the service.

Table 10: ADC Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
ADC State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	ADCE

Table 10: ADC Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
ADC Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 1 = Errors	✓	✓	ADCA
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✗	✓	N/A
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "Administrative Domain Controller"	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A

Table 10: ADC Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
System Status					
Service Load	Percent	Percentage of the CPU time used by this service; indicating how busy the service is.	✓	✓	N/A
Memory Usage	Bytes	RAM currently being used by this service.	✓	✓	N/A
Percent Memory Used	Percent	Percent of total available RAM being used. This can be greater than 100% if disk swap space is used.	✓	✓	PMEM
Service Uptime	Duration	Total duration since the last restart.	✗	✓	N/A
Service Runtime	Duration	Total duration the service has functioned since installation; the sum of all uptimes.	✗	✓	N/A
Restarts	Count	Total number of restarts since installation.	✓	✓	N/A
Reference Clock Source	Text	Indicates the origin of timing information; used for audit messages, communication, and timing functions: • NTP • GPS (not used in the HPMA)	✗	✓	N/A
Reference Clock Status	Enumerated Text	Indicates the current condition of the timing source: 0 = Stable 1 = Flywheeling 2 = Unstable 3 = Offline 4 = Unknown	✓	✓	TRFS

Table 10: ADC Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Local Clock Status	Enumerated Text	Indicates the condition of the internal timing system: 0 = Calibrating 1 = Synchronizing 2 = Syntonizing 3 = Flywheeling (Recalibrating) 4 = Flywheeling	✓	✓	TRSS
Local Clock Rate Error	ppm	The error between the local clock and the reference clock.	✓	✓	N/A
Local Clock Rate Drift	ppm	The cumulative offsets (since last restart) required by the local clock to keep in sync with the reference clock.	✓	✓	N/A
Network Neighbor Drift	µs	Rough measure of how different this service's clock is from that of the ADC services.	✓	✓	TNER

ADC Components

The only component supported by the ADC is the Connectivity component.

Connectivity

The ADC Connectivity component supports the standard set of network attributes.

Table 11: ADC ▶ Connectivity Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	bits / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	bits / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A

Table 11: ADC ▶ Connectivity Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Transmitted Bytes	Bytes	Total data sent since the last restart.	✓	✓	N/A
Connectivity Status					
Connected ADCs	Count	Number of ADC services connected to this service.	✓	✓	NADC
Connected NMSs	Count	Number of NMS services connected to this service.	✓	✓	NNMS
Audit Message Destinations	Count	Number of services that can accept audit messages from this service.	✓	✓	NAMS
Audit Messages Queued	Count	Messages waiting for confirmed delivery to an AMS (or audit relay service).	✓	✓	AMQS
Audit Messages Committed	Count	Messages committed to the AMS (or audit relay service).	✓	✓	N/A
Connections					
Node ID	Number	Unique node ID of a connected service.	✗	✗	N/A
User Label	Text	User-defined label for the connected service. If the label appears blue, this service has a connection to it, but the NMS does not.	✗	✗	N/A
Status	Text	Connection status of the service: • Connected • Reconnecting Transient service connections disappear from the list when disconnected. Only retained service connections can report "Reconnecting" when the connection is lost.	✗	✗	N/A

AMS—Audit Management System

The Audit Management System (AMS) logs all audited system events to a text file on the server. The grid uses positive acknowledgement to prevent loss of audit messages. A message remains queued at a service until the AMS, or an intermediate audit relay service, has acknowledged control of it.

Access to the audit log files is limited to authorized technical support staff unless you have purchased the audit option. For those with the audit option a separate document detailing access and log content is provided.

AMS Attributes

The AMS supports the common set of service attributes. These common service attributes appear on the Overview tab for the service.

Table 12: AMS Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
AMS State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	AUME
AMS Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 1 = DB Connectivity Error	✓	✓	AUMA
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✗	✓	N/A

Table 12: AMS Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "Audit Management System".	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A
System Status					
Service Load	Percent	Percentage of the CPU time used by this service; indicating how busy the service is.	✓	✓	N/A
Memory Usage	Bytes	RAM currently being used by this service.	✓	✓	N/A
Percent Memory Used	Percent	Percent of total available RAM being used. This can be greater than 100% if disk swap space is used.	✓	✓	PMEM
Service Uptime	Duration	Total duration since the last restart.	✗	✓	N/A

Table 12: AMS Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Service Runtime	Duration	Total duration the service has functioned since installation; the sum of all uptimes.	✗	✓	N/A
Restarts	Count	Total number of restarts since installation.	✓	✓	N/A
Reference Clock Source	Text	Indicates the origin of timing information; used for audit messages, communication, and timing functions: • NTP • GPS (not used in the HPMA)	✗	✓	N/A
Reference Clock Status	Enumerated Text	Indicates the current condition of the timing source: 0 = Stable 1 = Flywheeling 2 = Unstable 3 = Offline 4 = Unknown	✓	✓	TRFS
Local Clock Status	Enumerated Text	Indicates the condition of the internal timing system: 0 = Calibrating 1 = Synchronizing 2 = Syntonizing 3 = Flywheeling (Recalibrating) 4 = Flywheeling	✓	✓	TRSS
Local Clock Rate Error	ppm	The error between the local clock and the reference clock.	✓	✓	N/A
Local Clock Rate Drift	ppm	The cumulative offsets (since last restart) required by the local clock to keep in sync with the reference clock.	✓	✓	N/A
Network Neighbor Drift	µs	Rough measure of how different this service's clock is from that of the ADC services.	✓	✓	TNER

AMS Components

In addition to the standard service attributes, the AMS also supports the following components:

- Events
- Connectivity

Events

This component reports audit message statistics.

The Events component ensures that every audit message is accounted for and tracked. The message totals listed are cumulative from the last restart of the AMS service.

Table 13: AMS ▶ Events Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Connectivity Status	Enumerated Text	The status of the AMS connectivity to its database: 0 = Connecting 1 = Connected 2 = Connectivity Lost, Reconnecting 3 = Database Authentication Failed, Retrying Not used in the HP Medical Archive.	✓	✓	ERRS
Audit Messages Received	Count	Messages received by the AMS since the last restart.	✓	✓	N/A
Audit Message Receive Rate	Messages / second	Rate of incoming audit messages.	✓	✓	N/A
Audit Messages Queued	Count	Messages queued to be written to the log file.	✓	✓	AMQS
Audit Messages Committed	Count	Messages written to the log file (since the last restart).	✓	✓	N/A

Table 13: AMS ▶ Events Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Audit Message Commit Rate	Messages / second	Rate of message commitment to the log file.	✓	✓	N/A

Connectivity

The AMS supports a subset of the standard Connectivity component attributes (audit message attributes are handled in the events component).

Table 14: AMS ▶ Connectivity Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	bits / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	bits / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A
Transmitted Bytes	Bytes	Total data sent since the last service restart.	✓	✓	N/A
Connectivity Status					
Connected ADCs	Count	Number of ADC services connected to this service.	✓	✓	NADC
Connected NMSs	Count	Number of NMS services connected to this service.	✓	✓	NNMS
Connections					
Node ID	Number	Unique node ID of a connected service.	✗	✗	N/A
User Label	Text	User-defined label for the connected service. If the label appears blue, this service has a connection to it, but the NMS does not.	✗	✗	N/A

Table 14: AMS ▶ Connectivity Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Status	Text	Connection status of the service: • Connected • Reconnecting Transient service connections disappear from the list when disconnected. Only retained service connections can report "Reconnecting" when the connection is lost.	✘	✘	N/A

CLB—Connection Load Balancer

The Connection Load Balancer (CLB) directs incoming content to the most optimal storage service based on a variety of criteria. The CLB ranks nodes based on several factors such as availability, and system load. When the most optimal node has been chosen, the CLB establishes an outgoing connection and forwards the traffic to the chosen node.

The CLB serves as a connection pipeline between the remote entity and an LDR for DICOM.

CLB Attributes

The CLB supports the common set of service attributes. These common service attributes appear on the Overview tab for the service.

Table 15: CLB Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
CLB State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	CLBE
CLB Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 10 = Errors	✓	✓	CLBA
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✗	✓	N/A

Table 15: CLB Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "Connection Load Balancer"	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A
System Status					
Service Load	Percent	Percentage of the CPU time used by this service; indicating how busy the service is.	✓	✓	N/A
Memory Usage	Bytes	RAM currently being used by this service.	✓	✓	N/A
Percent Memory Used	Percent	Percent of total available RAM being used. This can be greater than 100% if disk swap space is used.	✓	✓	PMEM
Service Uptime	Duration	Total duration since the last restart.	✗	✓	N/A

Table 15: CLB Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Service Runtime	Duration	Total duration the service has functioned since installation; the sum of all uptimes.	✗	✓	N/A
Restarts	Count	Total number of restarts since installation.	✓	✓	N/A
Reference Clock Source	Text	Indicates the origin of timing information; used for audit messages, communication, and timing functions: • NTP • GPS (not used in the HPMA)	✗	✓	N/A
Reference Clock Status	Enumerated Text	Indicates the current condition of the timing source: 0 = Stable 1 = Flywheeling 2 = Unstable 3 = Offline 4 = Unknown	✓	✓	TRFS
Local Clock Status	Enumerated Text	Indicates the condition of the internal timing system: 0 = Calibrating 1 = Synchronizing 2 = Syntonizing 3 = Flywheeling (Recalibrating) 4 = Flywheeling	✓	✓	TRSS
Local Clock Rate Error	ppm	The error between the local clock and the reference clock.	✓	✓	N/A
Local Clock Rate Drift	ppm	The cumulative offsets (since last restart) required by the local clock to keep in sync with the reference clock.	✓	✓	N/A
Network Neighbor Drift	µs	Rough measure of how different this service's clock is from that of the ADC services.	✓	✓	TNER

CLB Components

In addition to the standard service attributes, the CLB also supports the following components:

- DICOM
- HTTP
- Connectivity

DICOM

DICOM is optional on the HPMA.

The DICOM component handles forwarding of DICOM traffic to optimal services and tracks TCP/IP connectivity for DICOM connections. The number of available destinations for query and retrieval (Q/R) and for ingest via DICOM are reported, as are statistics on connections.

Table 16: CLB ▶ DICOM Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Destinations					
Number Available Q/R Destinations	Count	Nodes accepting DICOM connections for content query and retrieve operations.	✓	✓	CAQD
Number Available Ingest Destinations	Count	Nodes that accept DICOM connections for ingesting content to the grid.	✓	✓	CAID
DICOM Associations					
Currently Established Incoming Associations	Count	Active associations originated from remote entities, to the grid.	✓	✓	N/A
Currently Established Outgoing Associations	Count	Active associations originated from the grid, to remote entities.	✓	✓	N/A
Incoming Associations - Attempted	Count	Attempted associations from remote entities since the last restart.	✓	✓	N/A

Table 16: CLB ▶ DICOM Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Incoming Associations - Successful	Count	Attempted associations from remote entities that succeeded in connecting at the TCP/IP layer (since the last restart).	✓	✓	N/A
Incoming Associations - Failed	Count	Attempted associations from remote clients that failed to connect at the TCP/IP layer (since the last restart).	✓	✓	CIAF
Incoming Associations - Refused	Count	Attempted associations that were refused by all grid destinations (since the last restart).	✓	✓	N/A
Incoming Associations - Failed Node Side	Count	Associations from remote entities that connected and then failed due to a TCP/IP problem in the grid (since the last restart).	✓	✓	N/A
Incoming Associations - Failed Client Side	Count	Associations from remote entities that connected and then failed due to a TCP/IP problem at the remote entity (since the last restart).	✓	✓	N/A
Incoming Associations - Unknown Failure	Count	Attempted associations from remote entities that failed to connect the TCP/IP layer for unknown reasons (since the last restart).	✓	✓	N/A
Outgoing Associations - Attempted	Count	Attempted associations from the grid since the last restart.	✓	✓	N/A
Outgoing Associations - Successful	Count	Attempted associations from the grid that succeeded in connecting at the TCP/IP layer (since the last restart).	✓	✓	N/A
Outgoing Associations - Failed	Count	Attempted associations from the grid that failed to connect at the TCP/IP layer (since the last restart).	✓	✓	COAF

Table 16: CLB ▶ DICOM Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Outgoing Associations - Refused	Count	Attempted associations from the grid that were refused by the remote destination (since the last restart).	✓	✓	N/A
Outgoing Associations - Failed Node Side	Count	Associations from the grid that connected and then failed due to a TCP/IP problem in the grid (since the last restart).	✓	✓	N/A
Outgoing Associations - Failed Client Side	Count	Associations from the grid that connected and then failed due to a TCP/IP problem at the remote entity (since the last restart).	✓	✓	N/A
Outgoing Associations - Unknown Failure	Count	Attempted associations from the grid that failed to connect the TCP/IP layer for unknown reasons (since the last restart).	✓	✓	N/A

HTTP

The FSG uses HTTP for grid transactions.

The HTTP component handles forwarding of HTTP session traffic to optimal services and tracks TCP/IP connectivity for HTTP connections. The number of available destinations for query and retrieval (Q/R) and for ingest via HTTP are reported, as are statistics on connections.

Table 17: CLB ▶ HTTP Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Destinations					
Number Available Q/R Destinations	Count	Nodes accepting HTTP connections for content query and retrieve operations.	✓	✓	CAQH
Number Available Ingest Destinations	Count	Nodes that accept HTTP connections for ingesting content to the grid.	✓	✓	CAIH

Table 17: CLB ▶ HTTP Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
HTTP Sessions					
Incoming Sessions - Established	Count	Active HTTP sessions originated from remote entities.	✓	✓	N/A
Incoming Sessions - Attempted	Count	Attempted sessions from remote entities at the TCP/IP layer (since the last restart).	✓	✓	N/A
Incoming Sessions - Successful	Count	Attempted sessions from remote clients that succeeded in connecting at the TCP/IP layer (since the last restart).	✓	✓	N/A
Incoming Sessions - Failed	Count	Attempted sessions from remote clients that failed to connect at the TCP/IP layer (since the last restart).	✓	✓	CISF
Incoming Sessions - Refused	Count	Attempted sessions that were refused by all grid destinations (since the last restart).	✓	✓	N/A
Incoming Sessions - Failed Node Side	Count	Sessions that connected and then failed due to a TCP/IP problem in the grid (since the last restart).	✓	✓	N/A
Incoming Sessions - Failed Client Side	Count	Sessions that connected and then failed due to a TCP/IP problem at the remote entity (since the last restart).	✓	✓	N/A
Incoming Sessions - Unknown Failure	Count	Attempted sessions that failed to connect the TCP/IP layer for unknown reasons (since the last restart).	✓	✓	N/A

Connectivity

The CLB supports the standard Connectivity component attributes.

Table 18: CLB ▶ Connectivity Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	bits / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	bits / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A
Transmitted Bytes	Bytes	Total data sent since the last restart.	✓	✓	N/A
Connectivity Status					
Connected ADCs	Count	Number of ADC services connected to this service.	✓	✓	NADC
Connected NMSs	Count	Number of NMS services connected to this service.	✓	✓	NNMS
Audit Message Destinations	Count	Number of services that can accept audit messages from this service.	✓	✓	NAMS
Audit Messages Queued	Count	Messages waiting for confirmed delivery to an AMS (or audit relay service).	✓	✓	AMQS
Audit Messages Committed	Count	Messages committed to the AMS (or audit relay service).	✓	✓	N/A
Connections					
Node ID	Number	Unique node ID of a connected service.	✗	✗	N/A
User Label	Text	User-defined label for the connected service. If the label appears blue, this service has a connection to it, but the NMS does not.	✗	✗	N/A

Table 18: CLB ▶ Connectivity Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Status	Text	Connection status of the service: • Connected • Reconnecting Transient service connections disappear from the list when disconnected. Only retained service connections can report "Reconnecting" when the connection is lost.	✘	✘	N/A

CMN—Configuration Management Node

This service provides a mechanism to perform grid-wide configuration of connectivity and protocol features needed by all services in the grid. Viewing the attributes of this service and its components, enables you to determine:

- The File System Gateway (FSG) replication groups (see page 102) and the roles each FSG is performing.
- The remote entities permitted to connect and to which capabilities they have access
- The state and history of Grid Tasks; specially programmed operations to update or service the HP Medical Archive.
- Your Grid ID number
- Other information related to servicing your grid.

Remote Connections and Permissions

Components of this service control the list of "friends" from which connections to the grid are permitted. Each of these is allocated permission to use the HTTP or DICOM protocol, or both. Within each protocol, there are profiles that govern the permitted activities.

Access to the settings for components of this service is restricted to the Vendor account. Contact HP technical support for assistance.

CMN Attributes

The CMN supports the standard set of service attributes. These common service attributes appear on the Overview tab for the service.

Table 19: CMN Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
CMN State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	CMNE

Table 19: CMN Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
CMN Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 1 = Error	✓	✓	CMNA
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✗	✓	N/A
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "Configuration Management Node".	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A

Table 19: CMN Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
System Status					
Service Load	Percent	Percentage of the CPU time used by this service; indicating how busy the service is.	✓	✓	N/A
Memory Usage	Bytes	RAM currently being used by this service.	✓	✓	N/A
Percent Memory Used	Percent	Percent of total available RAM being used. This can be greater than 100% if disk swap space is used.	✓	✓	PMEM
Service Uptime	Duration	Total duration since the last restart.	✗	✓	N/A
Service Runtime	Duration	Total duration the service has functioned since installation; the sum of all uptimes.	✗	✓	N/A
Restarts	Count	Total number of restarts since installation.	✓	✓	N/A
Reference Clock Source	Text	Indicates the origin of timing information; used for audit messages, communication, and timing functions: • NTP • GPS (not used in the HPMA)	✗	✓	N/A
Reference Clock Status	Enumerated Text	Indicates the current condition of the timing source: 0 = Stable 1 = Flywheeling 2 = Unstable 3 = Offline 4 = Unknown	✓	✓	TRFS

Table 19: CMN Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Local Clock Status	Enumerated Text	Indicates the condition of the internal timing system: 0 = Calibrating 1 = Synchronizing 2 = Syntonizing 3 = Flywheeling (Recalibrating) 4 = Flywheeling	✓	✓	TRSS
Local Clock Rate Error	ppm	The error between the local clock and the reference clock.	✓	✓	N/A
Local Clock Rate Drift	ppm	The cumulative offsets (since last restart) required by the local clock to keep in sync with the reference clock.	✓	✓	N/A
Network Neighbor Drift	µs	Rough measure of how different this service's clock is from that of the ADC services.	✓	✓	TNER

CMN Components

In addition to the standard service attributes, the CMN also supports the following components:

- Audit
- IP Ranges
- HTTP
- HTTP Advanced
- DICOM
- DICOM Advanced
- DICOM Indexes
- FSG Groups
- Grid Options
- Grid Tasks
- NMS Entities
- Connectivity

Access to the settings for components of this service is restricted to the Vendor account. Contact HP technical support for assistance.

Audit

This component provides data on the level of audit message reporting to the audit log. The audit log is a file of grid events used by technical support staff when troubleshooting issues.

Access to the audit log files is limited to authorized technical support staff unless you have purchased the audit option. For those with the audit option a separate document detailing access and log content is provided.

Table 20: CMN ▶ Audit Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Audit Levels					
Audit Category	Text	Categories of grid events that can generate audit messages.	✘	✓	N/A
Level	Enumerated Text	The level of audit messages that are retained in the audit log: 0 = Off (none) 1 = Error 2 = Normal 3 = Debug	✘	✓	N/A
Audit Category Code	Text	A four-character code designation for the class of audit messages. Not applicable to the HP Medical Archive.	✘	✓	N/A

IP Ranges

This component provides data on the range of IP addresses from which the grid will accept a TCP/IP connection.

IP ranges are organized by an IP Range Name; usually a geographical location, a device, or a workgroup of users. The Location and group assignments are not used in the HP Medical Archive.

If an incoming IP address is included in more than one range, the device is matched to the first occurrence from the top of the table downward.

The protocols supported for entities connecting from an address in the range are indicated by check boxes.

Table 21: CMN ▶ IP Ranges Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Allowable IP Ranges					
IP Range Name	Text	User-defined label assigned to the IP range, usually a location or workgroup.	✘	✓	N/A
IP Range	Dotted decimal or CIDR	Range of remote IP addresses (inclusive) from which the grid accepts TCP/IP connections.	✘	✓	N/A
Location	Text	Case sensitive reference to an entry in the Locations table below.	✘	✓	N/A
DICOM	Check box	Indicates if DICOM protocol is supported for devices in this IP range.	✘	✓	N/A
HTTP	Check box	Indicates if HTTP is supported for devices in this IP range.	✘	✓	N/A
Locations					
Location	Text	User-defined name for a location definition; this is referenced in the IP Ranges table.	✘	✓	N/A
X Coordinate	Meters	This is not used in the HP Medical Archive; leave blank.	✘	✓	N/A
Y Coordinate	Meters		✘	✓	N/A
Z Coordinate	Meters		✘	✓	N/A
Group ID	Number	This is not used in the HP Medical Archive; leave blank.	✘	✓	N/A

HTTP

When a range of IP addresses defined above has HTTP support enabled, those devices must also be enabled as HTTP entities using this component. This allocates a capability profile (see "HTTP Advanced" below) to the devices from selected IP ranges.

Table 22: CMN ▶ HTTP Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
HTTP Entities					
Description	Text	User-defined description for the set of entities in this IP range.	✘	✓	N/A
IP Range	Dotted decimal or CIDR	Range of remote device IP addresses (inclusive) to which the grid assigns the profile.	✘	✓	N/A
Profile Name	Text	Case sensitive reference to an entry defined in the HTTP Advanced component. The profile governs the permitted activities for connections from this IP range.	✘	✓	N/A

HTTP Advanced

Each remote entity that supports HTTP is allocated a profile defining the capabilities the grid offers to that entity. This component defines the profiles that can be assigned in the HTTP component (above).

Profiles can be defined in each of the three supported namespaces:

- /CBID for object access by Content Block ID
- /UUID for access by Universal Unique ID handle
- /DICOM for adding DICOM content to the grid

The range of capabilities HTTP offers in each namespace varies. The same (case sensitive) profile name can be repeated in each namespace.

Thus, a profile combines capabilities for an entity to use more than one namespace.

Table 23: CMN ▶ HTTP Advanced Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
HTTP /CBID Namespace					
Profile Name	Text	User-defined profile name. This name is referenced in the HTTP component.	✘	✓	N/A
PUT	Check box	Indicates if clients assigned this profile can use the HTTP PUT command to add content to the grid.	✘	✓	N/A
GET	Check box	Indicates if clients assigned this profile can use the HTTP GET command to retrieve content from the grid.	✘	✓	N/A
POST	Check box	Indicates if clients assigned this profile can use the HTTP POST (query) command.	✘	✓	N/A
DELETE	Check box	Indicates if clients assigned this profile can use the HTTP DELETE command; disabled in this release.	✘	✓	N/A
HTTP /UUID Namespace					
Profile Name	Text	User-defined profile name. This name is referenced in the HTTP component.	✘	✓	N/A
PUT	Check box	Indicates if clients assigned this profile can use the HTTP PUT command to store files and allocate a UUID handle.	✘	✓	N/A
GET	Check box	Indicates if clients assigned this profile can use the HTTP GET command to retrieve files by UUID handle; disabled in this release.	✘	✓	N/A

Table 23: CMN ▶ HTTP Advanced Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
POST	Check box	Indicates if clients assigned this profile can use the HTTP POST (query) command; disabled in this release.	✘	✓	N/A
DELETE	Check box	Indicates if clients assigned this profile can use the HTTP DELETE command to release a UUID handle.	✘	✓	N/A
HTTP /DICOM Namespace					
Profile Name	Text	User-defined profile name. This name is referenced in the HTTP component.	✘	✓	N/A
AE Title	Text	The AE Title allocated to the remote entity.	✘	✓	N/A
Coerce Tag Profile Name	Text	Case sensitive reference to an entry defined in the DICOM Advanced component. The profile is used to enable data partitioning.	✘	✓	N/A
PUT	Check box	Indicates if remote entities assigned this profile can use the HTTP PUT command to store DICOM objects. This should always be enabled; without it, an entity with this profile has no access to the DICOM namespace.	✘	✓	N/A

DICOM

DICOM is optional on the HPMA.

When a range of IP addresses defined above has DICOM support enabled, devices from that range must also be enabled as DICOM Application Entities (AEs). This allocates a capability profile (see "DICOM Advanced" below) to those devices. An entity is uniquely defined by the combination of AE Title, IP address and port, and the grid AE to which it is associating. For example, entities can share an AE Title and port number while still being distinguished by unique IP addresses within the defined range.

The grid can present multiple AE titles, so associations must also match the caller to an accepted grid AE. This is used to assign differing profiles to single remote AEs.

Table 24: CMN ▶ DICOM Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
DICOM AEs					
Description	Text	User-defined description of the entity or group of entities.	✘	✓	N/A
AE Title	Text	The AE Title of the remote entity.	✘	✓	N/A
IP Range	Dotted decimal or CIDR	A remote device IP address (or inclusive range) to which the grid assigns the profile.	✘	✓	N/A
Port	Number	The port used for DICOM by the remote device.	✘	✓	N/A
Via LDR	Check box	Indicates whether the LDR can make direct connections with remote entities. If *not* selected, connections are routed through a CLB service. The HP Medical Archive must use the CLB (check box is deselected).	✘	✓	N/A
GRID AE	Text	AE Title of the grid to which the entity can associate.	✘	✓	N/A
Profile Name	Text	Case sensitive reference to an entry defined in the DICOM Advanced component. The profile governs the permitted activities for entities in this IP range.	✘	✓	N/A

DICOM Advanced

Each remote entity that supports DICOM can be allocated a profile defining the capabilities the grid offers to that entity. This component defines the profiles that can be assigned to AEs in the DICOM component (above).

The Advanced Config Profile is used during the association handshake to control the types of actions permitted and the format of files in the

transfer syntax. Some entities present problems when a particular action (SOP class) or transfer syntax is used. If an Advanced Config Profile is applied, the grid enforces a complex rule set on the association.

Table 25: CMN ▶ DICOM Advanced Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
DICOM Profiles					
Profile Name	Text	User-defined name for this profile. This name is referenced in the DICOM component.	✘	✓	N/A
S	Check box	Send to GRID—indicates an entity with this profile can store DICOM files to the grid.	✘	✓	N/A
R	Check box	Receive from GRID—indicates an entity with this profile can retrieve DICOM files from the grid.	✘	✓	N/A
F	Check box	Find on GRID—indicates an entity with this profile can issue query commands for DICOM content.	✘	✓	N/A
M	Check box	Move—indicates an entity with this profile can issue a DICOM command for the grid to open another association to relay an object.	✘	✓	N/A
C	Check box	Commit Storage—indicates an entity with this profile can query for acknowledgement that an object was stored.	✘	✓	N/A
Max # Concurrent Associations	Number	Maximum number of simultaneous associations permitted to an entity in this profile; used to prevent overloading the remote entity at times of high traffic volume.	✘	✓	N/A
Coerce Tag Profile Name	Text	This is not used in the HP Medical Archive; leave blank.	✘	✓	N/A

Table 25: CMN ▶ DICOM Advanced Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Advanced Config Profile Name	Text	Case sensitive reference to an entry defined in the Advanced Config Profiles table of the DICOM Advanced component. The profile dictates rules to apply when hand-shaking the association.	✘	✓	N/A
Coerce Tag Profiles					
This table is unused in the HP Medical Archive. It applies only to enterprise installations.					
Advanced Config Profiles					
Advanced Configura-tion Profile Name	Text	User-defined name for the advanced configuration profile. This name is referenced by the DICOM Profiles above.	✘	✓	N/A
Behavior	Text	Indicates whether to allow or disallow a particular SOP Class action during an association: • Allow • Disallow	✘	✓	N/A
SOP Class	DICOM standard string	Class (action) to which the Behavior applies. This may be an asterisk "*" indicating "all classes".	✘	✓	N/A
Preferred Transfer Syntax	DICOM standard string	Preferred format for images. See "Advanced Config Profiles" on page 286 for details.	✘	✓	N/A
Required Transfer Syntax	DICOM standard string	Format required in a request. See "Advanced Config Profiles" on page 286 for details.	✘	✓	N/A

DICOM Indexes

This component provides a list of the DICOM tags that are used by the grid for query and content management. This information is read-only and cannot be altered through the NMS interface.

Table 26: CMN ▶ DICOM Indexes Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
DICOM Indexed Tags					
Label	Text	Description of the tag's purpose; its use.	✘	✘	N/A
Extracted Tag	Text	DICOM standard tag designation.	✘	✘	N/A

FSG Groups

For each FSG (File System Gateway) service within the grid, this component lists:

- The replication group to which the service belongs; indicating which services are mirrors to provide redundancy within the grid.
- Whether the service is the default primary (the gateway for remote entities) or a secondary (mirror) service.
- Whether a secondary service has been forced to act as a primary; a failover condition while a default primary service is being serviced.

Table 27: CMN ▶ FSG Groups Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
File System Gateway Groups					
FSG Node ID	Number	Unique node ID of a connected FSG service.	✘	✓	N/A
FSG Replication Group	Number	Arbitrary (non-zero) number used to associate FSG services into a group; a primary gateway and secondary mirrors.	✘	✓	N/A
Default Primary	Check box	Indicates whether the service is the default primary within the replication group.	✘	✓	N/A

Table 27: CMN ▶ FSG Groups Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Forced Primary	Check box	Indicates whether the service is operating as a primary while the default primary is unavailable. Normally this is not checked; the service is in its normal role.	✘	✓	N/A

Grid Options

This component provides information about your grid deployment.

Table 28: CMN ▶ Grid Options Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Grid Information					
Grid ID	Text	A unique identifier for your grid deployment, needed to configure expansion nodes.	✘	✓	N/A
Configured	Date and time	A timestamp indicating when your grid configuration was created by the manufacturer. This date changes as new nodes are added to the configuration.	✘	✓	N/A

Grid Tasks

This component monitors the status of grid-wide programmed maintenance tasks. When exceptional maintenance is required—adding new node certificates for example—a special Grid Task program is entered and run. Preparing and running Grid Tasks is an HP technical support activity. The Overview tab for this component displays information about these Grid Tasks.

Table 29: CMN ▶ Grid Tasks Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Pending Tasks	Count	Number of Grid Tasks that have been entered into the system but not yet started running.	✓	✓	N/A

Table 29: CMN ▶ Grid Tasks Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Active Tasks	Count	Number of Grid Tasks that are actively running.	✓	✓	N/A
Aborted Tasks	Count	Number of Grid Tasks that were aborted by the user.	✓	✓	N/A
Failed Tasks	Count	Number of Grid Tasks that failed to complete due to encountered errors.	✓	✓	N/A
Completed Tasks	Count	Number of Grid Tasks that have been completed successfully.	✓	✓	N/A
Last Task Message	Text	Most recently received message from a Grid Task indicating a task stage completion, task failure, pause, or abort.	✗	✓	N/A
Pending					
Task ID	Number	Identifier assigned when the task is generated.	✗	✗	N/A
Description	Text	Brief description of the task; its purpose.	✗	✗	N/A
Valid From	Date and time	Time stamp when the task becomes valid. It cannot be successfully activated before this time.	✗	✗	N/A
Valid To	Date and time	Time stamp after which the task is no longer valid and cannot be started. If the task is active when at this time, it continues to execute normally.	✗	✗	N/A
Source	Text	The author of the task.	✗	✗	N/A
Active					
Task ID	Number	Identifier assigned when the task is generated.	✗	✗	N/A
Description	Text	Brief description of the task; its purpose.	✗	✗	N/A

Table 29: CMN ▶ Grid Tasks Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Start Time	Date and time	Time stamp when the task first became active.	✘	✘	N/A
Duration	HH:MM:SS	Elapsed time since the task was first activated.	✘	✘	N/A
Status	Text	Current status of the task; one of: Active—currently running Paused—manually paused Abort Rollback—processing a manual abort Paused Abort Rollback—manually paused an abort Failure Rollback—recovering from a failure Paused Failure Rollback—manually paused a failure rollback	✘	✘	N/A
Stage	Text	Description of the currently executing stage of the task.	✘	✘	N/A
Historical					
Task ID	Number	Identifier assigned when the task is generated.	✘	✘	N/A
Description	Text	Brief description of the task; its purpose.	✘	✘	N/A
Start Time	Date and time	Time stamp when the task first became active.	✘	✘	N/A
Completion Time	Date and time	Time stamp when the task moved to the Historical list.	✘	✘	N/A
Result	Text	Description of why the task is now historical.	✘	✘	N/A

NMS Entities

This component provides information about entities shown in the NMS interface. The NMS interface presents the names of entities above

the service level (nodes, cabinets, sites, and grid) in several locations. Settings in this component determine:

- The name that appears, based on the selected language of the user account that logs in
- The sequence that entities appear in the navigation tree

At this time only English is supported.

Names are allocated to each entity by using a system of Object IDs (OIDs) that are unique to each entity while being hierarchically organized. Each row in the NMS Entities table allocates a name in a specified language to an entity OID. The combination of OID hierarchy and position in the table determines the sequence of appearance in the navigation tree.

Table 30: CMN ▶ NMS Entities Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
NMS Entities					
OID		A unique identifier for an entity of your grid deployment.	✗	✓	N/A
Name	Text	A user defined name for the entity in the Language selected.	✗	✓	N/A
Language	Text	The language designation of the Name for an entity OID.	✗	✓	N/A

Connectivity

The CMN supports the standard Connectivity component attributes.

Table 31: CMN ▶ Connectivity Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	bits / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	bits / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A
Transmitted Bytes	Bytes	Total data sent since the last restart.	✓	✓	N/A

Table 31: CMN ▶ Connectivity Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Connectivity Status					
Connected ADCs	Count	Number of ADC services connected to this service.	✓	✓	NADC
Connected NMSs	Count	Number of NMS services connected to this service.	✓	✓	NNMS
Audit Message Destinations	Count	Number of services that can accept audit messages from this service.	✓	✓	NAMS
Audit Messages Queued	Count	Messages waiting for confirmed delivery to an AMS (or audit relay service).	✓	✓	AMQS
Audit Messages Committed	Count	Messages committed to the AMS (or audit relay service).	✓	✓	N/A
Connections					
Node ID	Number	Unique node ID of a connected service.	✗	✗	N/A
User Label	Text	User-defined label for the connected service. If the label appears blue, this service has a connection to it, but the NMS does not.	✗	✗	N/A
Status	Text	Connection status of the service: • Connected • Reconnecting Transient service connections disappear from the list when disconnected. Only retained service connections can report "Reconnecting" when the connection is lost.	✗	✗	N/A

CMS—Content Management System

While the LDR manages the payload content on the grid, the Content Management System (CMS) provides the logic. The CMS is a distributed database that maintains a map of all HP Medical Archive system content and its associated metadata (such as media type and DICOM-specific information).

System content is managed by the CMS according to business rules. The CMS tracks content and manages data duplication to maximize system and data availability. With multiple distributed CMS nodes, you are protected against system failures and have constant access to grid data.

The CMS also manages access to the grid's data. When a content request is made, the CMS works with the ADC to determine which is the most optimal node from which to deliver that content. This ensures that data is delivered in a timely and optimized manner. Once an LDR receives approval from the CMS, it releases the content.

An SQL database is used to support queries on the payload metadata. The CMS maintains this database and responds to queries.

CMS Attributes

The CMS supports a subset of the standard set of service attributes for state, status, and node information. It excludes the service status section attributes entirely.

Table 32: CMS Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
CMS State	Text	Current state of the service; always "Online" in this release.	✓	✓	N/A
CMS Status	Text	Always reports "No Errors" in this release.	✓	✓	N/A
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A

Table 32: CMS Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Notes	Text	Additional user-defined text providing description and annotations for the service or server.	✗	✓	N/A
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "Content Management System".	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A

CMS Components

In addition to the standard service attributes, the CMS also supports the following components:

- Content
- Database
- DICOM
- Synchronization
- Connectivity

Content

This component reports statistics on the grid payload and replication activity.

Table 33: CMS ▶ Content Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Content	Count	Number of objects stored in the grid.	✓	✓	N/A
Ingest Overview					
New Content	Count	Number of new objects being processed through the business rules for replication.	✓	✓	DCiN
Information Lifecycle Management					
ILM Implementation	Text	Name for the business rules package currently in force.	✗	✓	N/A
ILM Version	Text	Version number of the business rules package.	✗	✓	N/A
Content Replication					
Active Replications	Count	Objects in the process of being replicated.	✓	✓	N/A
Scheduled Replications	Count	Objects scheduled for re-evaluation at a later time.	✓	✓	N/A
Replication Rate	Objects / second[1]	Rate at which objects are currently being replicated.	✓	✓	N/A

Table 33: CMS ▶ Content Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Replications	Count	Total object replications by this CMS service since startup.	✓	✓	N/A
Content Purging					
Purge Rate	Objects / second[1]	Rate at which unneeded objects are deleted, as determined by business rules.	✓	✓	N/A
Purges	Number	Unneeded objects deleted.	✓	✓	N/A

1 Rates are calculated by tracking the last five events. The elapsed time over all five events is converted into events per second.

Database

This component provides information about the type of database used by the CMS for metadata tracking, and data transaction statistics with that database. Each addition and each query to the database are considered transactions.

General database statistics include the number of transactions to date, the data transaction rate, and the number of connections to the database.

Table 34: CMS ▶ Database Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Type	Text	The name of the database software being used; typically “mysql”, and “InnoDB”. If these values appear otherwise, the grid configuration may need correction.	✗	✓	N/A
Engine	Text		✗	✓	N/A
Database Statistics					
Transactions	Count	Total number of database operations since the last restart.	✓	✓	N/A
Transaction Rate	Transactions / second[1]	Number of database operations per second.	✓	✓	N/A

Table 34: CMS ▶ Database Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Connections	Count	Number of open database connections.	✓	✓	N/A
InnoDB Tablespace					
Allocated Tablespace	Bytes	The amount of disk space allocated to the metadata database.	✓	✓	N/A
Free Tablespace	Bytes	The amount of space remaining in the metadata database.	✓	✓	DBSF

1 Rates are calculated by tracking the last five events. The elapsed time over all five events is converted into events per second.

DICOM

DICOM is optional on the HPMA.

This component of the CMS reports on managed DICOM content.

Table 35: CMS ▶ DICOM Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Studies	Count	Total unique DICOM studies managed by the system. Note that duplicates are identified by a full match of DICOM study tags. If some tags are missing or different, the study is considered unique. This may lead to a higher number than expected.	✓	✓	N/A
Instances	Count	Total DICOM instances (images) managed by the system, excluding duplicates.	✓	✓	N/A

Synchronization

The Synchronization component provides information on message processing and data transmission dating back to the day the CMS was first started. The Synchronization component is useful for viewing detailed statistics about the rate that data is being processed and sent

from the CMS, as well as determining whether the CMS is operating efficiently and data is being processed in a timely manner.

Table 36: CMS ▶ Synchronization Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Incoming Messages	Count	Estimated number of synchronization messages that the CMS must process to be fully synchronized.	✓	✓	CsQL
Incoming Message Processing Rate	Messages / second[1]	Rate that synchronization messages are being received.	✓	✓	N/A
Queue Size	Count	Outgoing synchronization messages queued to be sent to other CMSs.	✓	✓	CsQT
Processing					
Message Processing Rate	Messages / second[1]	Rate that synchronization messages are processed.	✓	✓	N/A
Messages Processed	Count	Total synchronization messages processed since the last restart.	✓	✓	N/A
Data Processing Rate	bits / second[1]	Rate that synchronization message data is being processed.	✓	✓	N/A
Data Processed	Bytes	Total number of synchronized message bytes received since the last restart of the service.	✓	✓	N/A
Sending					
Message Sending Rate	Messages / second[1]	Rate that outgoing synchronization messages are being generated.	✓	✓	N/A
Messages Sent	Count	Total synchronization messages generated since the last restart, excluding those in the queue.	✓	✓	N/A
Data Sending Rate	bits / second[1]	Transmission rate of synchronization message data.	✓	✓	N/A

Table 36: CMS ▶ Synchronization Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Data Sent	Bytes	Total number of synchronized message bytes sent since the last restart, excluding the queue.	✓	✓	N/A

1 Rates are calculated by tracking the last five events. The elapsed time over all five events is converted into events per second.

Connectivity

The CMS supports the standard Connectivity component attributes with the addition of the number of connected CMSs, and without the status of connected nodes (assumed to be online).

Table 37: CMS ▶ Connectivity Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	bits / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	bits / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A
Transmitted Bytes	Bytes	Total data sent since the last restart.	✓	✓	N/A
Connectivity Status					
Connected ADCs	Count	Number of ADC services connected to this service.	✓	✓	NADC
Connected CMSs	Count	Number of additional CMS services connected to this service (not including the service itself); related to synchronization.	✓	✓	NCMS
Connected NMSs	Count	Number of NMS services connected to this service.	✓	✓	NNMS
Audit Message Destinations	Count	Number of services that can accept audit messages from this service.	✓	✓	NAMS

Table 37: CMS ▶ Connectivity Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Audit Messages Queued	Count	Messages waiting for confirmed delivery to an AMS (or audit relay service).	✓	✓	AMQS
Audit Messages Committed	Count	Messages committed to the AMS (or audit relay service).	✓	✓	N/A
Connections					
Node ID	Number	Unique node ID of a connected service.	✗	✗	N/A
User Label	Text	User-defined label for the connected service. If the label appears blue, this service has a connection to it, but the NMS does not.	✗	✗	N/A

FSG—File System Gateway

The File System Gateway (FSG) provides a virtual file system interface using CIFS (Windows) or NFS (Unix/Linux). This allows any type of fixed content, such as lab results, doctors notes, audio, video, and diagnostic images, to be stored on the grid. This enables the sharing of imaging studies between numerous applications. Specifically, all Picture Archiving and Communication Systems (PACS) can seamlessly store and retrieve images on the grid without the need for proprietary interfaces.

The HP Medical Archive has two FSG services paired in the base replication group. The Primary FSG provides the normal gateway access into the grid for read and write operations. The Secondary FSG provides a “mirror” of the file system and is used to generate daily backups. The Secondary FSG supports read-only gateway access.

There can be up to two replication groups in the HP Medical Archive (base and expansion). The nodes used to host the Secondary FSG vary based on the type of deployment, Single Site or Single Site + DR.

Table 38: FSG Host Nodes

Single Site	Primary FSG	Secondary FSG
Base Group	GN1-A-1	AN1-A-1
Expansion Group	GN1-A-2	GN2-A-2
Single Site + DR	**Primary FSG**	**Secondary FSG**
Base Group	GN1-A-1	GN1-B-1
Expansion Group	GN1-A-2	GN1-B-2

The Secondary FSG automatically stores a backup of the managed file system into the grid each day. Activity that takes place after the backup is retained as a “replication session”. Both the Primary and Secondary retain the replication session messages.

FSG Attributes

The FSG supports the standard set of service attributes for state, status, and node information.

Table 39: FSG Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
FSG State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	FGWE
FSG Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 1 = Waiting for CMSs 2 = Starting 3 = Shutting Down	✓	✓	FGWA
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✗	✓	N/A
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "File System Gateway".	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A

Table 39: FSG Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A
System Status					
Service Load	Percent	Percentage of the CPU time used by this service; indicating how busy the service is.	✓	✓	N/A
Memory Usage	Bytes	RAM currently being used by this service.	✓	✓	N/A
Percent Memory Used	Percent	Percent of total available RAM being used. This can be greater than 100% if disk swap space is used.	✓	✓	PMEM
Service Uptime	Duration	Total duration since the last restart.	✗	✓	N/A
Service Runtime	Duration	Total duration the service has been functioning since installation; the sum of all uptimes.	✗	✓	N/A
Restarts	Count	Total number of restarts since installation.	✓	✓	N/A
Reference Clock Source	Text	Indicates the origin of timing information; used for audit messages, communication, and timing functions: • NTP • GPS (not used in the HPMA)	✗	✓	N/A

Table 39: FSG Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Reference Clock Status	Enumerated Text	Indicates the current condition of the timing source: 0 = Stable 1 = Flywheeling 2 = Unstable 3 = Offline 4 = Unknown	✓	✓	TRFS
Local Clock Status	Enumerated Text	Indicates the condition of the internal timing system: 0 = Calibrating 1 = Synchronizing 2 = Syntonizing 3 = Flywheeling (Recalibrating) 4 = Flywheeling	✓	✓	TRSS
Local Clock Rate Error	ppm	The error between the local clock and the reference clock.	✓	✓	N/A
Local Clock Rate Drift	ppm	The cumulative offsets (since last restart) required by the local clock to keep in sync with the reference clock.	✓	✓	N/A
Network Neighbor Drift	µs	Rough measure of how different this service's clock is from that of the ADC services.	✓	✓	TNER

FSG Components

In addition to the standard service attributes, the FSG also supports the following components:

- Storage
- Replication
- Backup
- Client Services
- Connectivity

Storage

As files are ingested through the FSG, they are cached locally and forwarded to the grid for persistent storage. The FSG maintains the file system directory tree locally. Payload data is stored in the grid, making the file system appear to have very high capacity, even though the FSG server itself has relatively modest local resources.

This component provides data on the service's storage space, and the objects cached and processed.

Table 40: FSG ▶ Storage Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Total Cache	Bytes	Total storage space on the server allocated for caching data going to and from the grid.	✓	✓	N/A
Total Cache Available	Bytes	Total local cache space currently available (unused).	✓	✓	FSTA
Percent Total Cache Available	Percent	Percentage of total local cache space that is still available for use.	✓	✓	N/A
File System Operations					
Cached Files	Count	Number of files cached at the FSG server.	✓	✓	N/A
Create Operations	Count	Number of new files or folders created in the file system directory tree since the last service restart.	✓	✓	N/A
Read Operations	Count	Total read operations executed on the local disk since the last service restart; a rough indicator of service activity.	✓	✓	N/A
Write Operations	Count	Total write operations executed on the local disk since the last service restart; a rough indicator of service activity.	✓	✓	N/A
Read Operation Rate	Transactions / second	Rate at which disk read operations are currently being executed on the local disk.	✓	✓	N/A

Table 40: FSG ▶ Storage Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Write Operation Rate	Transactions / second	Rate at which disk write operations are currently being executed on the local disk.	✓	✓	N/A
Store To Grid					
Files Stored to Grid - Pending	Count	Number of new files cached locally, waiting for transfer to the grid for persistent storage.	✓	✓	FSGP
Files Stored to Grid - Attempted	Count	Number of file transfers initiated to the grid.	✓	✓	N/A
Files Stored to Grid - Successful	Count	Number of file transfers completed successfully; stored persistently on to the grid.	✓	✓	N/A
Files Stored to Grid - Retrying	Count	Number of file transfers that failed and are actively being retried.	✓	✓	FSGR
Files Stored to Grid - Retries	Count	Accumulated number of retries needed to ingest content to the grid, since last restart.	✓	✓	N/A
File Store Rate	Transactions / second	Rate at which files are successfully stored to the grid.	✓	✓	N/A
Retrieve From Grid					
Files Retrieved from Grid - Pending	Count	Number of file retrieval requests waiting for the grid to respond.	✓	✓	FRGP
Files Retrieved from Grid - Attempted	Count	Number of file retrieval requests issued to the grid.	✓	✓	N/A
Files Retrieved from Grid - Successful	Count	Number of files successfully retrieved from the grid.	✓	✓	N/A

Table 40: FSG ▶ Storage Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Files Retrieved from Grid - Retrying	Count	Number of file retrieval requests that failed and are being retried.	✓	✓	FRGR
Files Retrieved from Grid - Retries	Count	Accumulated number of retries needed to retrieve content from the grid, since last restart.	✓	✓	N/A
Files Retrieved from Grid - Failed	Count	Accumulated number of failures to retrieve content from the grid, since last restart.	✓	✓	FRGF
File Retrieved Rate	Transactions / second	Rate at which files are successfully retrieved from the grid.	✓	✓	N/A
Remove From Grid					
File Remove Notifications	Count	Number of objects deleted from the file system. The CMS is notified of the deletion; actual object purging depends on business rules within the CMS.	✓	✓	N/A
File Remove Rate	Transactions / second	Rate at which file deletion notifications are being sent to the grid.	✓	✓	N/A
DICOM					
DICOM Objects Detected	Count	Not used by the HP Medical Archive.	✓	✓	N/A
Part 10 Validation Failures	Count	Not used by the HP Medical Archive.	✓	✓	FDPP

Replication

This component reports information about the replication status of the service. The grid supports mirror FSG services to provide failover support should a primary FSG service become unavailable.

The sections for Primary and Secondary are populated with data based on the role of this FSG service; if acting as a Primary, the Secondary section contains no meaningful data and vice versa.

Table 41: FSG ▶ Replication Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Configured Role	Enumerated Text	Assigned role for the FSG service at system configuration: 0 = Primary 1 = Secondary	✓	✓	N/A
Current Role	Enumerated Text	Current role of the FSG service: 0 = Primary 1 = Secondary 2 = Rebuild	✓	✓	N/A
Replication Status	Enumerated Text	Current status of the replication module of the FSG: 0 = Normal 1 = No Primary 2 = Error	✓	✓	RSTU
FSG Group ID	Number	Arbitrary (non-zero) number used to associate FSG services into a group; a primary gateway and secondary mirrors.	✗	✓	N/A
Primary FSG Node ID	Number	Unique node ID of the designated primary FSG service within this group.	✗	✓	N/A
Primary					
Active Session ID	Number	Unique identifier of the current replication session to which messages are being appended.	✗	✓	N/A
Next Operation Identifier	Number	Sequence number for the next transaction to be added to this replication session.	✗	✓	N/A
Enqueued Messages	Count	Accumulated count of replication messages generated since the last service restart.	✗	✓	N/A

Table 41: FSG ▶ Replication Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Connected Secondaries	Count	Number of currently connected secondary FSG services within this group.	✗	✓	N/A
Secondary					
Active Session ID	Number	Unique identifier of the current replication session from which messages are being processed.	✗	✓	N/A
Next Operation Identifier	Number	Sequence number for the next transaction to be processed from this replication session.	✗	✓	N/A
Dequeued Messages	Count	Accumulated count of replication messages processed since the last service restart.	✗	✓	N/A
Pending Operations	Count	Approximate count of replication messages to be processed in the current session. This is the sum of unprocessed messages at this FSG and an approximate number of messages in the queue at the primary.	✗	✓	SPOP

Backup

This component provides information about backups of the managed file system. The FSG is configured at installation to make regular backup copies of the file system (folder and file information) and ingest them into the grid. Should the shared file system become corrupted, a backup can be used to restore the system. Restoration from a backup requires technical expertise; it is a technical support maintenance activity.

Table 42: FSG ▶ Backup Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Successful Backups	Count	Number of successful backups since last restart.	✓	✓	N/A

Table 42: FSG ▶ Backup Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Failed Backups	Count	Number of failed backups since last restart.	✓	✓	N/A
Backup Schedule					
Next Scheduled Backup	Timestamp	Date and time of next scheduled backup. The schedule is determined at grid installation.	✗	✓	N/A
Backup Frequency	Text	"Daily" by default, the actual frequency is determined by installation settings for days of the week, and dates of the month.	✗	✓	N/A
Backup Start Window	Time	Time when backup can begin.	✗	✓	N/A
Backup End Window	Time	Time, after which a backup cannot begin. A backup in progress may continue after this time. If this is the same as the Backup Start Window, backup is disabled.	✗	✓	N/A
Current Backup					
Current Status	Enumerated Text	Current status of the backup process: 0 = Active 1 = Idle	✓	✓	N/A
Start Time	Time	Time stamp when the current backup started.	✗	✓	N/A
Percentage Complete	Percent	Indicator of current backup progress.	✗	✓	N/A
Previous Backup					
Backup Result	Enumerated Text	Indicator the result of the previous backup process: 0 = Successful 1 = Failure	✓	✓	PBST
Start Time	Time	Time stamp when the last backup started.	✗	✓	N/A

Table 42: FSG ▶ Backup Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
End Time	Time	Time stamp when the last backup ended.	✘	✓	N/A
Backup Identifier	Number	Unique identifier of the backup session.	✘	✓	N/A
Number of Objects	Count	Number of objects included in the last backup.	✘	✓	N/A

Client Services

This component provides information about the support services used to manage the file system share (NFS, CIFS). If this service is not running, you do not have access to the grid's managed file system.

Table 43: FSG ▶ Client Services Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Client Services State	Enumerated Text	Current state of the service: 3 = Stopping... 2 = Running 1 = Starting... 0 = Stopped	✓	✓	N/A
Client Services Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 10 = Client Service Error	✓	✓	FCSA
Client Services					
Service Name	Text	The name of a file sharing service.	✘	✓	N/A
Status	Enumerated Text	The status of the file sharing service.	✘	✓	N/A

Connectivity

The FSG supports the standard Connectivity component attributes.

Table 44: FSG ▶ Connectivity Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	bits / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	bits / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A
Transmitted Bytes	Bytes	Total data sent since the last restart.	✓	✓	N/A
Connectivity Status					
Connected ADCs	Count	Number of ADC services connected to this service.	✓	✓	NADC
Connected NMSs	Count	Number of NMS services connected to this service.	✓	✓	NNMS
Audit Message Destinations	Count	Number of services that can accept audit messages from this service.	✓	✓	NAMS
Audit Messages Queued	Count	Messages waiting for confirmed delivery to an AMS (or audit relay service).	✓	✓	AMQS
Audit Messages Committed	Count	Messages committed to the AMS (or audit relay service).	✓	✓	N/A
Connections					
Node ID	Number	Unique node ID of a connected service.	✗	✗	N/A
User Label	Text	User-defined label for the connected service. If the label appears blue, this service has a connection to it, but the NMS does not.	✗	✗	N/A

Table 44: FSG ▶ Connectivity Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Status	Text	Connection status of the service: • Connected • Reconnecting Transient service connections disappear from the list when disconnected. Only retained service connections can report "Reconnecting" when the connection is lost.	✘	✘	N/A

LDR—Local Distribution Router

The Local Distribution Router (LDR) handles content transport on the grid. Content transport encompasses many tasks including data storage, routing, and request handling. The LDR does the majority of the grid's hard work by handling the heavy data transfer loads and the extensive data traffic functions.

The LDR handles the following tasks:

- Content storage
- Content caching
- Content transfers from another LDR
- Data storage management
- Protocol interfaces (DICOM and HTTP)

LDR Attributes

The LDR supports all the standard service attributes plus additional attributes for component state and status, and a system status entry for open file descriptors.

Table 45: LDR Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
LDR State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	LDRE
LDR Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 1 = Waiting for CMSs 2 = Shutting Down	✓	✓	LDRA
Storage State	Enumerated Text	Current state of the Storage component of the service: 0 = Offline 1 = Standby 2 = Verify 3 = Online (Read Only) 4 = Online	✓	✓	SSTE

Table 45: LDR Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Storage Status	Enumerated Text	The status of the Storage component's functionality: 0 = No Errors 1 = Not Started 2 = Performing Startup Checks 3 = Inaccessible 4 = Crosscheck Failed 5 = Corrupt 6 = Verify Local Synchronize Failed 7 = Max Failures Reached 8 = Insufficient Free Space 9 = Unknown Error	✓	✓	SSTU
DICOM State	Enumerated Text	Current state of the DICOM interface component: 0 = Offline 1 = Redirect 2 = Online (Read-Only) 3 = Online	✓	✓	MSTE
DICOM Status	Enumerated Text	The status of the DICOM component's functionality: 0 = No Errors 1 = Not Started 2 = Invalid/Missing DICOM Dictionary 3 = Starting... 4 = Stopping... 5 = Invalid/Missing Indexed Tag List 6 = Unknown Error	✓	✓	MSTU
HTTP State	Enumerated Text	Current state of the HTTP interface component: 0 = Offline 1 = Redirect 2 = Online (Read-Only) 3 = Online	✓	✓	HSTE

Table 45: LDR Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
HTTP Status	Enumerated Text	The status of the HTTP component's functionality: 0 = No Errors 2 = Not Started 3 = Starting... 4 = Stopping...	✓	✓	HSTU
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✗	✓	N/A
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "Local Distribution Router".	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A

Table 45: LDR Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
System Status					
Service Load	Percent	Percentage of the CPU time used by this service; indicating how busy the service is.	✓	✓	N/A
Memory Usage	Bytes	RAM currently being used by this service.	✓	✓	N/A
Percent Memory Used	Percent	Percent of total available RAM being used. This can be greater than 100% if disk swap space is used.	✓	✓	PMEM
Open File Descriptors	Number	A measure of operating system resources in use. This is monitored to ensure that key resources are being released when not needed.	✓	✓	FOPN
Service Uptime	Duration	Total duration since the last restart.	✗	✓	N/A
Service Runtime	Duration	Total duration the service has functioned since installation; the sum of all uptimes.	✗	✓	N/A
Restarts	Count	Total number of restarts since installation.	✓	✓	N/A
Reference Clock Source	Text	Indicates the origin of timing information; used for audit messages, communication, and timing functions: • NTP • GPS (not used in the HPMA)	✗	✓	N/A
Reference Clock Status	Enumerated Text	Indicates the current condition of the timing source: 0 = Stable 1 = Flywheeling 2 = Unstable 3 = Offline 4 = Unknown	✓	✓	TRFS

Table 45: LDR Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Local Clock Status	Enumerated Text	Indicates the condition of the internal timing system: 0 = Calibrating 1 = Synchronizing 2 = Syntonizing 3 = Flywheeling (Recalibrating) 4 = Flywheeling	✓	✓	TRSS
Local Clock Rate Error	ppm	The error between the local clock and the reference clock.	✓	✓	N/A
Local Clock Rate Drift	ppm	The cumulative offsets (since last restart) required by the local clock to keep in sync with the reference clock.	✓	✓	N/A
Network Neighbor Drift	µs	Rough measure of how different this service's clock is from that of the ADC services.	✓	✓	TNER

LDR Components

In addition to the standard service attributes, the LDR also supports the following components:

- Storage
- DICOM
- HTTP
- Connectivity

Storage

This component provides information on the object storage space and the objects processed. The Storage component tracks the total amount of object storage space being used and the space available. If the available space falls below the configured amount, a warning alarm state

occurs. This allows you to manage the storage proactively and purchase additional capacity only when necessary.

Table 46: LDR ▶ Storage Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Storage State	Enumerated Text	Current state of the Storage component of the service: 0 = Offline 1 = Standby 2 = Verify 3 = Online (Read Only) 4 = Online	✓	✓	SSTE
Storage Status	Enumerated Text	The status of the Storage component's functionality: 0 = No Errors 1 = Not Started 2 = Performing Startup Checks 3 = Inaccessible 4 = Crosscheck Failed 5 = Corrupt 6 = Verify Local Synchronize Failed 7 = Max Failures Reached 8 = Insufficient Free Space 9 = Unknown Error	✓	✓	SSTU
Total Space	Bytes	Total storage space allocated to all object stores.	✓	✓	N/A
Total Space Available	Bytes	Total object storage space currently available (unused).	✓	✓	N/A
Percent Total Space Available	Percent	Percentage of object storage space that is still available for use.	✓	✓	SAVP
Total Persistent Data	Bytes	Size of the persistently stored data.	✓	✓	N/A
Total Cached Data	Bytes	Size of the transient (cached) data; used for system optimization.	✓	✓	N/A
Block Reads	Count	Total read operations executed on the disk storage system; indicating how busy the disk is.	✓	✓	N/A

Table 46: LDR ▶ Storage Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Block Writes	Count	Total write operations executed on the disk storage system; indicating how busy the disk is.	✓	✓	N/A
Objects Retrieved	Count	Persistent objects retrieved from the storage system of this service.	✓	✓	N/A
Objects Committed	Count	Persistent objects stored on the storage system of this service.	✓	✓	N/A
Objects Purged	Count	Persistent objects purged from the storage system of this service.	✓	✓	N/A
Background Verification					
Objects Verified	Count	Objects that the background verifier has checked for consistency.	✓	✓	N/A
Bytes Verified	Bytes	Total number of bytes the background verifier has checked.	✓	✓	N/A
Corrupt Objects Detected	Count	Objects that failed verification; can indicate disk corruption or data tampering.	✓	✓	OCOR
Object Stores					
ID	ID number	Identifier of an object store. The component can support multiple stores.	✗	✗	N/A
Total	Bytes	Total space in the object store.	✗	✗	N/A
Available	Bytes	Total space currently available (unused) in the store.	✗	✗	N/A
Stored Data	Bytes	Size of the persistently stored data in the object store.	✗	✗	N/A
(%)	Percentage	Percentage of store currently in use for persistent data.	✗	✗	N/A
Cached Data	Bytes	Size of the transient (cached) data stored in the object store.	✗	✗	N/A
(%)	Percentage	Percentage of store that is in use for cached data.	✗	✗	N/A

DICOM

DICOM is optional on the HPMA.

The DICOM component tracks connectivity over the DICOM interface and statistics on DICOM transactions.

Table 47: LDR ▶ DICOM Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
DICOM State	Enumerated Text	Current state of the DICOM interface component: 0 = Offline 1 = Redirect 2 = Online (Read-Only) 3 = Online Redirection transparently routes DICOM associations to other LDR services.	✓	✓	MSTE
DICOM Status	Enumerated Text	The status of the DICOM component's functionality: 0 = No Errors 1 = Not Started 2 = Invalid/Missing DICOM Dictionary 3 = Starting... 4 = Stopping... 5 = Invalid/Missing Indexed Tag List 6 = Unknown Error	✓	✓	MSTU
DICOM Associations					
Currently Established Incoming Associations	Count	Current DICOM associations initiated remotely (by users or other grid services).	✓	✓	N/A
Currently Established Outgoing Associations	Count	Current DICOM associations initiated by this service.	✓	✓	N/A

Table 47: LDR ▶ DICOM Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Incoming Associations - Attempted	Count	Counters of all incoming DICOM associations attempted, the ones that were accepted, and those that failed. Failures are monitored for alarms. Counters are reset when the DICOM component is restarted; goes from offline to online.	✓	✓	N/A
Incoming Associations - Successful	Count		✓	✓	N/A
Incoming Associations - Failed	Count		✓	✓	DEIA
Outgoing Associations - Attempted	Count	Counters of all outgoing DICOM associations that this service attempted, the ones that were accepted, and those that failed. Failures are monitored for alarms. Counters are reset when the DICOM component is restarted; goes from offline to online.	✓	✓	N/A
Outgoing Associations - Successful	Count		✓	✓	N/A
Outgoing Associations - Failed	Count		✓	✓	DEOA

Table 47: LDR ▶ DICOM Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
DICOM C-ECHO					
Inbound C-Echoes - Attempted	Count	Counters of all attempted, successful, and failed DICOM C-Echo commands. Both inbound and outbound statistics are tracked. Failures are monitored for alarms. Counters reset when the DICOM component is restarted; goes from offline to online.	✓	✓	N/A
Inbound C-Echoes - Successful	Count		✓	✓	N/A
Inbound C-Echoes - Failed	Count		✓	✓	DEAE
Outbound C-Echoes - Attempted	Count		✓	✓	N/A
Outbound C-Echoes - Successful	Count		✓	✓	N/A
Outbound C-Echoes - Failed	Count		✓	✓	DEEO

Table 47: LDR ▶ DICOM Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
DICOM C-STORE					
Inbound C-Stores - Attempted	Count	Counters of all attempted, successful, and failed DICOM C-Store commands. Both inbound and outbound statistics are tracked. Failures are monitored for alarms. Counters are reset when the DICOM component is restarted; goes from offline to online.	✓	✓	N/A
Inbound C-Stores - Successful	Count		✓	✓	N/A
Inbound C-Stores - Failed	Count		✓	✓	DEAI
Outbound C-Stores - Attempted	Count		✓	✓	N/A
Outbound C-Stores - Successful	Count		✓	✓	N/A
Outbound C-Stores - Failed	Count		✓	✓	DEAO
DICOM C-FIND					
Inbound C-Finds - Attempted	Count	Counters of all attempted, successful, and failed DICOM C-Find commands. Only inbound statistics are tracked; the service does not issue C-Find commands. Failures are monitored for alarms. Counters are reset when the DICOM component is restarted; goes from offline to online.	✓	✓	N/A
Inbound C-Finds - Successful	Count		✓	✓	N/A
Inbound C-Finds - Failed	Count		✓	✓	DEAF

Table 47: LDR ▶ DICOM Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
DICOM C-MOVE					
Inbound C-Moves - Attempted	Count	Counters of all attempted, successful, and failed DICOM C-Move commands. Only inbound statistics are tracked; the service does not issue C-Move commands. Failures are monitored for alarms. Counters are reset when the DICOM component is restarted; goes from offline to online.	✓	✓	N/A
Inbound C-Moves - Successful	Count		✓	✓	N/A
Inbound C-Moves - Failed	Count		✓	✓	DEAM
DICOM Storage Commitment					
Inbound Storage Commitment - Attempted	Count	Counters of all attempted, successful, and failed DICOM Storage Commitment confirmation requests. Only inbound statistics are tracked; the service does not issue Commit queries. Failures are monitored for alarms. Counters are reset when the DICOM component is restarted; goes from offline to online.	✓	✓	N/A
Inbound Storage Commitment - Successful	Count		✓	✓	N/A
Inbound Storage Commitment - Failed	Count		✓	✓	DESC

HTTP

The HTTP component tracks connectivity over the HTTP interface and statistics on HTTP transactions. The FSG uses the HTTP interface for transactions with the grid content.

Table 48: LDR ▶ HTTP Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
HTTP State	Enumerated Text	Current state of the HTTP interface component: 0 = Offline 1 = Redirect 2 = Online (Read-Only) 3 = Online Redirection transparently routes HTTP sessions to other LDR services.	✓	✓	HSTE
HTTP Status	Enumerated Text	The status of the HTTP component's functionality: 0 = No Errors 2 = Not Started 3 = Starting... 4 = Stopping...	✓	✓	HSTU
HTTP Sessions					
Currently Established Incoming Sessions	Count	Current HTTP sessions.	✓	✓	N/A
Incoming Sessions - Attempted	Count	Counters of all incoming HTTP sessions attempted, those that were accepted, and those that failed. Counters are reset when the HTTP component is restarted; goes from offline to online.	✓	✓	N/A
Incoming Sessions - Successful	Count		✓	✓	N/A
Incoming Sessions - Failed	Count		✓	✓	HEIS

Table 48: LDR ▶ HTTP Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
HTTP GET					
Inbound GETs - Attempted	Count	Counters of all attempted, successful, and failed GET commands to retrieve content. Counters are reset when the HTTP component is restarted; goes from offline to online.	✓	✓	N/A
Inbound GETs - Successful	Count		✓	✓	N/A
Inbound GETs - Failed	Count		✓	✓	HEIG
HTTP PUT					
Inbound PUTs - Attempted	Count	Counters of all attempted, successful, and failed PUT commands to store content. Counters are reset when the HTTP component is restarted; goes from offline to online.	✓	✓	N/A
Inbound PUTs - Successful	Count		✓	✓	N/A
Inbound PUTs - Failed	Count		✓	✓	HEIP
HTTP POST					
Inbound POSTs - Attempted	Count	Counters of all attempted, successful, and failed POST commands to query content. Counters are reset when the HTTP component is restarted; goes from offline to online.	✓	✓	N/A
Inbound POSTs - Successful	Count		✓	✓	N/A
Inbound POSTs - Failed	Count		✓	✓	HEIT

Table 48: LDR ▶ HTTP Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
HTTP HEAD					
Inbound HEADs - Attempted	Count	Counters of all attempted, successful, and failed HEAD commands to retrieve content metadata. Counters are reset when the HTTP component is restarted; goes from offline to online.	✓	✓	N/A
Inbound HEADs - Successful	Count		✓	✓	N/A
Inbound HEADs - Failed	Count		✓	✓	HEIH
HTTP DELETE					
Inbound DELETEs - Attempted	Count	Counters of all attempted, successful, and failed DELETE commands to delete content from the grid. Counters are reset when the HTTP component is restarted; goes from offline to online.	✓	✓	N/A
Inbound DELETEs - Successful	Count		✓	✓	N/A
Inbound DELETEs - Failed	Count		✓	✓	HEID
HTTP OPTION					
Inbound OPTIONs - Attempted	Count	Counters of all attempted, successful, and failed OPTION commands to query supported operations on an object. Counters are reset when the HTTP component is restarted; goes from offline to online.	✓	✓	N/A
Inbound OPTIONs - Successful	Count		✓	✓	N/A
Inbound OPTIONs - Failed	Count		✓	✓	HEIO

Connectivity

The LDR supports the standard Connectivity component attributes plus attributes for CMS connectivity.

Table 49: LDR ▶ Connectivity Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	bits / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	bits / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A
Transmitted Bytes	Bytes	Total data sent since the last restart.	✓	✓	N/A
Connectivity Status					
Connected ADCs	Count	Number of ADC services connected to this service.	✓	✓	NADC
Connected NMSs	Count	Number of NMS services connected to this service.	✓	✓	NNMS
Number of Available CMSs	Count	Number of CMS services connected to this service.	✓	✓	NCMS
CMS Timeouts	Count	Number of messages that timed out on the way to a CMS	✓	✓	N/A
Audit Message Destinations	Count	Number of services that can accept audit messages from this service.	✓	✓	NAMS
Audit Messages Queued	Count	Messages waiting for confirmed delivery to an AMS (or audit relay service).	✓	✓	AMQS
Audit Messages Committed	Count	Messages committed to the AMS (or audit relay service).	✓	✓	N/A

Table 49: LDR ▶ Connectivity Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Connections					
Node ID	Number	Unique node ID of a connected service.	✘	✘	N/A
User Label	Text	User-defined label for the connected service. If the label appears blue, this service has a connection to it, but the NMS does not.	✘	✘	N/A
Status	Text	Connection status of the service: • Connected • Reconnecting Transient service connections disappear from the list when disconnected. Only retained service connections can report "Reconnecting" when the connection is lost.	✘	✘	N/A

NMS—Network Management System

This document is a guide to the Network Management System (NMS). It performs two primary functions:

- It is a monitoring system that notifies you of problems when the status of key hardware or software changes.
- It is a browser-based interface making the system easily available to multiple users for:
  - Reporting status information about the grid so you can monitor and resolve grid issues.
  - Creating, viewing, and printing reports on current and historic data about each grid component based on your selection of report criteria.
  - Configuring grid components and customizing the notification settings according to your criteria.

NMS Attributes

The NMS supports the standard set of service attributes for node information and system status.

Table 50: NMS Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
NMS State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	NSCE
NMS Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 10 = DB Connectivity Error	✓	✓	NSCA
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A

Table 50: NMS Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✗	✓	N/A
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "Network Management System".	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A
System Status					
Service Load	Percent	Percentage of the CPU time used by this service; indicating how busy the service is.	✓	✓	N/A
Memory Usage	Bytes	RAM currently being used by this service.	✓	✓	N/A
Percent Memory Used	Percent	Percent of total available RAM being used. This can be greater than 100% if disk swap space is used.	✓	✓	PMEM

Table 50: NMS Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Service Uptime	Duration	Total duration since the last restart.	✗	✓	N/A
Service Runtime	Duration	Total duration the service has functioned since installation; the sum of all uptimes.	✗	✓	N/A
Restarts	Count	Total number of restarts since installation.	✓	✓	N/A
Reference Clock Source	Text	Indicates the origin of timing information; used for audit messages, communication, and timing functions: • NTP • GPS (not used in the HPMA)	✗	✓	N/A
Reference Clock Status	Enumerated Text	Indicates the current condition of the timing source: 0 = Stable 1 = Flywheeling 2 = Unstable 3 = Offline 4 = Unknown	✓	✓	TRFS
Local Clock Status	Enumerated Text	Indicates the condition of the internal timing system: 0 = Calibrating 1 = Synchronizing 2 = Syntonizing 3 = Flywheeling (Recalibrating) 4 = Flywheeling	✓	✓	TRSS
Local Clock Rate Error	ppm	The error between the local clock and the reference clock.	✓	✓	N/A
Local Clock Rate Drift	ppm	The cumulative offsets (since last restart) required by the local clock to keep in sync with the reference clock.	✓	✓	N/A
Network Neighbor Drift	µs	Rough measure of how different this service's clock is from that of the ADC services.	✓	✓	TNER

NMS Components

In addition to the standard service attributes, the NMS also supports the following components:

- Database
- Connectivity

Database

This component provides information about the type of database used by the NMS for attribute tracking.

Table 51: NMS ▶ Database Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Connectivity Status	Enumerated Text	The status of the service's functionality: 0 = Connecting... 1 = Connected 2 = Connection Lost, Reconnecting... 3 = Connection Timeout, Retrying... 4 = Authentication Failed, Retrying...	✓	✓	NDBC
Configuration					
Database Type	Text	The name of the database software being used; typically "mysql", version, and "InnoDB". If these values appear otherwise, the grid configuration may need correction.	✗	✓	N/A
Database Version	Text		✗	✓	N/A
Database Engine	Text		✗	✓	N/A
Tablespace					
Tablespace Allocated	Bytes	The amount of disk space allocated to the attribute history database.	✓	✓	N/A
Tablespace Available	Bytes	The amount of space remaining in the attribute history database.	✓	✓	NTBR

Connectivity

The NMS supports a subset of the standard Connectivity component attributes, and adds attributes for NMS connectivity.

Table 52: NMS ▶ Connectivity Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	bits / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	bits / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A
Transmitted Bytes	Bytes	Total data sent since the last restart.	✓	✓	N/A
Connectivity Status					
Connected ADCs	Number	Number of ADC services connected to this service.	✓	✓	NADC
Connected NMSs	Number	Number of NMS services connected to this service (including itself).	✓	✓	NNMS
Audit Message Destinations	Count	Number of services that can accept audit messages from this service.	✓	✓	NAMS
Audit Messages Queued	Count	Messages waiting for confirmed delivery to an AMS (or audit relay service).	✓	✓	AMQS
Audit Messages Committed	Count	Messages committed to the AMS (or audit relay service).	✓	✓	N/A
Connections					
Node ID	Number	Unique node ID of a connected service.	✗	✗	N/A
User Label	Text	User-defined label for the connected service.	✗	✗	N/A

Table 52: NMS ▶ Connectivity Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Status	Text	Connection status of the service: • Connected • Reconnecting Transient service connections disappear from the list when disconnected. Only retained service connections can report "Reconnecting" when the connection is lost.	✘	✘	N/A

SSM—Server Status Monitor

The Server Status Monitor (SSM) is a service present on *all* nodes. Each node on the grid has its own SSM to monitor that node's status, services, and the system log. It monitors the condition of the node and related hardware, polls the server and hardware drivers for information, and displays the processed data via the NMS interface.

The information monitored includes:

- CPU information (type, mode, speed)
- Memory information (available, used)
- Performance (system load, load average, uptime, restarts)
- Volumes (status, available space)

SSM Attributes

The SSM supports the standard set of service attributes for state, status, and Node Information only. System Status is replaced with a section on Server Status.

The full set of SSM service attributes are listed below.

Table 53: SSM Service Attributes

Attribute	Type / Units	Description	C	T	Alarm
SSM State	Enumerated Text	Current state of the service: 2 = Online 1 = Standby 0 = Offline	✓	✓	SSME
SSM Status	Enumerated Text	The status of the service's functionality: 0 = No Errors 10 = Error	✓	✓	SSMA
Node Information					
User Label	Text	User-defined label for the service appearing in the Navigation Tree, map views, and the title of the Content frame.	✗	✓	N/A

Table 53: SSM Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Notes	Text	Additional user-defined text providing description and annotations of the service or server.	✗	✓	N/A
Device Type	Text	The specific internal label for the service (allocated at manufacturing time), "Server Status Monitor".	✗	✓	N/A
Vendor	Text	Manufacturer of the service.	✗	✓	N/A
Version	Text	Code version and build information for the service. Reporting this can indicate when upgrades were implemented.	✗	✓	N/A
Node ID	Number	Unique node ID assigned at installation.	✗	✓	N/A
X Coordinate	Meters	Earth-Centered Earth-Fixed (ECEF) coordinates for the global position of the server. Not applicable to the HP Medical Archive.	✗	✓	N/A
Y Coordinate	Meters		✗	✓	N/A
Z Coordinate	Meters		✗	✓	N/A
Group ID	Number	Identifier of the logical group (location) to which the service belongs. Used in placing replications under business rules.	✗	✓	N/A
Server Status					
System Load	Percent	Percentage load; indicating how busy the computational processor of the server is for all services running.	✓	✓	N/A
System Load Average	Number	Provides a general measure of the load on the processor. High loads trigger an alarm.	✓	✓	SLSA
System Memory	Bytes	Total physical RAM on the server.	✓	✓	N/A

Table 53: SSM Service Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
System Memory Available	Bytes	Amount of free RAM on the server (excluding disk swap space).	✓	✓	UMEM
System Swap Memory Used	Bytes	Amount of virtual memory (disk swap space) being used.	✓	✓	SWMU
System Uptime	Duration	Total duration since the last server restart.	✗	✓	N/A
Restarts	Count	Total number of restarts since installation.	✓	✓	N/A
Processors					
Processor #	Number	Sequential count of processors installed in the server.	✗	✗	N/A
Processor Vendor	Text	Manufacturer of the processor.	✗	✗	N/A
Processor Type	Text	Processor model number.	✗	✗	N/A
Processor Speed	MHz	Clock speed of the processor.	✗	✗	N/A
Processor Cache	Bytes	Cache size of the processor.	✗	✗	N/A

SSM Components

In addition to the service attributes, the SSM also supports the following components:

- Events
- Volumes
- Services
- Network
- RAID

Events

This component relays logged events from the hardware drivers. Interpretation of these numbers depends on the hardware and drivers in use on your system. You can treat this data as a general indicator of problems with the server.

Table 54: SSM ▶ Events Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Log Monitor State	Enumerated Text	Indicates the state of the server's log monitor and its connection to the appropriate data file: 0 = Connected 1 = Initializing 2 = Bad Configuration 3 = Unable to Connect	✘	✓	SMST
Total Events	Count	The total number of logged error or fault events.	✓	✓	SMTT
Last Event	Text	Description of the last event detected by the server. This text is relayed verbatim from the server.	✘	✓	N/A

Table 54: SSM ▶ Events Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Error List					
IDE Errors	Count	Number of errors or faults as reported by the respective device drivers. Specific interpretation is dependent on the hardware and driver in use. These provide a general indicator of hardware faults or configuration issues. The counters can be reset individually via the Configuration page, and are reset whenever the server is restarted.	✘	✘	N/A
I/O Errors	Count		✘	✘	N/A
SCSI Errors	Count		✘	✘	N/A
File System Errors	Count		✘	✘	N/A
Network Receive Errors	Count		✘	✘	N/A
Network Transmit Errors	Count		✘	✘	N/A
Kernel Errors	Count		✘	✘	N/A
Kernel Memory Allocation Failure			✘	✘	N/A
Peer TCP Protocol Violations	Count		✘	✘	N/A

Resetting Error Event Counters

The error event counters can be individually reset to zero.

To reset error event counters:

1. Select the **SSM ▶ Events** component in the Navigation Tree.
2. Select the **Configuration ▶ Main** page.
3. Select the **Reset** column check boxes for specific event counters to be reset.
4. Click the **Apply** button to reset the checked counters.

Volumes

Information about mounted volumes on this server are reported.

Table 55: SSM ▶ Volumes Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Mount Point	Text	Local path of the mounted volume.	✘	✘	N/A
Status	Enumerated Text	Current status of the mounted volume: 0 = Unknown 1 = Offline 2 = Online	✘	✘	VMST
Size	Bytes	Size of the mounted volume.	✘	✘	N/A
Space Available	Bytes	Total available (unused) space on the volume.	✘	✘	VMFR
Entries Available	Number	A measure of how many more objects the volume can store (provided there is sufficient space).	✘	✘	VMFI

Services

This component tracks the services and support modules running on the node. It reports their status, the number of threads (CPU tasks) running and the amount of RAM being used. The grid services are listed, as are support modules (such as time synchronization).

The section on Packages reports overall service suite installations and version numbers to facilitate software update procedures.

Table 56: SSM ▶ Services Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Services					
Service	Text	Name of the monitored service.	✘	✘	N/A

Table 56: SSM ▶ Services Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Status	Enumerated Text	Indicates if the service is running or has been halted: 0 = Not Running 2 = Running	✘	✘	SVST
Threads	Number	Number of threads (CPU tasks) the module is currently running.	✘	✘	N/A
Memory	Bytes	RAM being used by the service or module.	✘	✘	N/A
Packages					
Package	Text	Name of a software suite package.	✘	✘	N/A
Installed	Text	Status of the package on this server (Installed or Not Installed)	✘	✘	N/A
Version	Text	Version number of the suite.	✘	✘	N/A

Network

This reports on the network adapter hardware and related drivers. Interpretation of the data is dependent on the hardware and driver in use. The attributes are listed below:

Table 57: SSM ▶ Network Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Received Data Rate	Bytes / s	Current rate that data is being received.	✓	✓	N/A
Transmitted Data Rate	Bytes / s	Current rate that data is being transmitted.	✓	✓	N/A
Received Bytes	Bytes	Total data received since the last service restart.	✓	✓	N/A
Transmitted Bytes	Bytes	Total data sent since the last restart.	✓	✓	N/A

Table 57: SSM ▶ Network Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Total Errors	Count	Sum of all errors that have occurred on all network interfaces since this service was started.	✓	✓	FERR
Devices					
Name	Text	Operating system name for the physical network port.	✗	✓	N/A
Label	Text	User-defined label for the port.	✗	✓	N/A
IP Address	Dotted decimal or CIDR	Address assigned at installation.	✗	✓	N/A
Speed	bits / s	Negotiated speed of the network connection as reported by the driver.	✗	✗	N/A
Duplex	Enumerated Text	Network Duplex setting reported by the driver: 0 = Full 1 = Half 2 = Unavailable 3 = Unknown 4 = Unsupported	✗	✗	NDUP
Auto Negotiate	Enumerated Text	Network Auto Negotiate setting reported by the driver. 0 = Off 1 = On 2 = Unavailable 3 = Unknown 4 = Unsupported For optimal performance, this must match your network's configuration requirements.	✗	✗	NANG
Link	Text	Connection to the network as reported by the driver.	✗	✗	NLNK
Receive					
Name	Text	Operating system name for the physical network port.	✗	✗	N/A

Table 57: SSM ▶ Network Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Bytes	Bytes	Received traffic since restart.	✘	✘	N/A
Packets	Count		✘	✘	N/A
Errors	Count	Driver reported fault counters. These may or may not be reported, and their interpretation varies, depending on the specific driver.	✘	✘	N/A
Dropped	Count		✘	✘	N/A
Frame Overruns	Count		✘	✘	N/A
Frames	Count		✘	✘	N/A
Transmit					
Name	Text	Operating system name for the physical network port.	✘	✘	N/A
Bytes	Bytes	Transmitted traffic since the last server restart.	✘	✘	N/A
Packets	Count		✘	✘	N/A
Errors	Count	Driver reported fault counters. These may or may not be reported, and their interpretation varies, depending on the specific driver.	✘	✘	N/A
Dropped	Count		✘	✘	N/A
Collisions	Count		✘	✘	N/A
Carrier	Count		✘	✘	N/A

RAID

This component only exists on SSMs that are directly monitoring at least one RAID unit. The RAID component displays extensive data on each attached RAID unit.

The NMS displays as much status and basic hardware information as each physical RAID communicates. This information includes the RAID controller status, the array status, and the status of each of the available drives.

Table 58: SSM ▶ RAID Component Attributes

Attribute	Type / Units	Description	C	T	Alarm
Monitor Status	Enumerated Text	The status of the connection between the SSM and the RAID monitoring driver: 0 = Connected 1 = Connecting... 2 = Disconnected	✓	✓	RMS1
Driver Version	Text	Revision and date reported by the RAID monitor driver.	✗	✗	N/A
Last Event	Text	Information about the last observed event on the RAID. Text is generated by the device and can have various values.	✗	✓	N/A
Controllers					
Controller	Number	Sequence number of the controller.	✗	✗	N/A
Vendor/ Model Name	Text	Manufacturer and model number of the RAID controller.	✗	✗	N/A
Firmware Revision	Text	Revision and date reported by the RAID controller firmware.	✗	✓	N/A
RAID Controller Status	Enumerated Text	Current status of the RAID controller: 0 = Online 1 = Offline	✓	✓	PATn
Enclosures					
Enclosure	Number	Sequence number of the drive enclosure.	✗	✗	N/A
Controller	Number	Sequence number of the controller from the table above.	✗	✗	N/A

Table 58: SSM ▶ RAID Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Fan Status	Enumerated Text	Current status of the RAID fan speed: 0 = OK 1 = Speed Low 2 = Speed High 3 = Stopped 4 = Failed 5 = Unavailable	✓	✓	PFAn
Temperature Status	Enumerated Text	Current status of the RAID temperature: 0 = OK 1 = Temp Low 2 = Temp High 3 = Critical 4 = Unavailable	✓	✓	PTEn
Power Supply Status	Enumerated Text	Current status of the RAID Voltage Regulator Module: 0 = No Errors 1 = VRM Removed 2 = VRM Failed 3 = Power Supply Fault 4 = Unavailable	✓	✓	PPSn
Arrays					
Array	Number	Sequence number of the array.	✗	✗	N/A
Controller	Number	Sequence number of the controller from the table above.	✗	✗	N/A
Drives	Number	Number of drives in the array.	✗	✗	N/A
Array Size	GB	Size of the configured storage array.	✗	✓	N/A
Array Type	Text	RAID level. An industry standard indicator of the type of RAID.	✗	✓	N/A
Array State	Enumerated Text	Current state of the array: 0 = Online 1 = Offline	✗	✓	PSAn

Table 58: SSM ▶ RAID Component Attributes (cont.)

Attribute	Type / Units	Description	C	T	Alarm
Array Status	Enumerated Text	Current status of the configured array: 0 = No Errors 1 = Rebuilding 2 = Ready to Rebuild 3 = Recovery Made 4 = Drive Fail 5 = Unknown Text is generated by the device and can have various values.	✘	✓	PSNn
Drives					
Slot	Number	Physical bay location of the drive.	✘	✘	N/A
Array	Number	Sequence number of the array in the table above.	✘	✘	N/A
Enclosure	Number	Sequence number of the drive enclosure in the table above.	✘	✘	N/A
Vendor/ Model Name	Text	Manufacturer and model number of the drive.	✘	✘	N/A
Size	GB	Total amount of storage on the drive.	✘	✘	N/A
Status	Enumerated Text	Current status of the drive: 0 = No Errors 1 = Rebuilding 2 = Missing 3 = Unknown 4 = Failed 5 = Spare 6 = Replaced	✘	✘	DSNn

Configuration 6

Alarms and Services

Customizing alarms and making changes to system configuration.

Chapter Contents

Introduction to Configuration 152

Alarm Configuration 153
- Configuration—Notification Page 153
- Active Alarms 155
- Changing Alarm Settings 157

Service and Component Configuration 158
- Configuration—Main Page 158
- ADC Configuration 159
- AMS Configuration 160
- CLB Configuration 160
- CMN Configuration 161
- CMS Configuration 162
- FSG Configuration 162
- LDR Configuration 164
- NMS Configuration 168
- SSM Configuration 168

Introduction to Configuration

The Network Management System provides functionality to configure general service functions, labels, operational settings, and the notification settings for alarms.

NOTICE

Access to the Configuration settings of the CMN service is restricted by User Account settings. Only the Vendor account can change settings in the CMN service.

WARNING

Changing configuration settings requires careful and deliberate planning. Some configurable elements can affect the state of your live system. Only experienced administrators should alter the device and component configuration settings.

CAUTION

Alarm settings are enabled as part of your grid installation. Changes to alarm settings should not be made for simple convenience; this may conceal underlying problems that should be resolved. If you find an alarm is persistent, discuss the situation with HP technical support before making changes.

Each service's Configuration tab has two pages:

- Main page—used to customize the service/component state and labels, and to reset some attribute counters. Service components may have additional configurable settings. The contents of this page are discussed for each service starting on page 159.
- Notification page—used to configure alarm settings. See "Alarm Configuration" below.

Alarm Configuration

Alarm settings have been made to suit the HP Medical Archive. Do not alter threshold settings without consulting HP technical support.

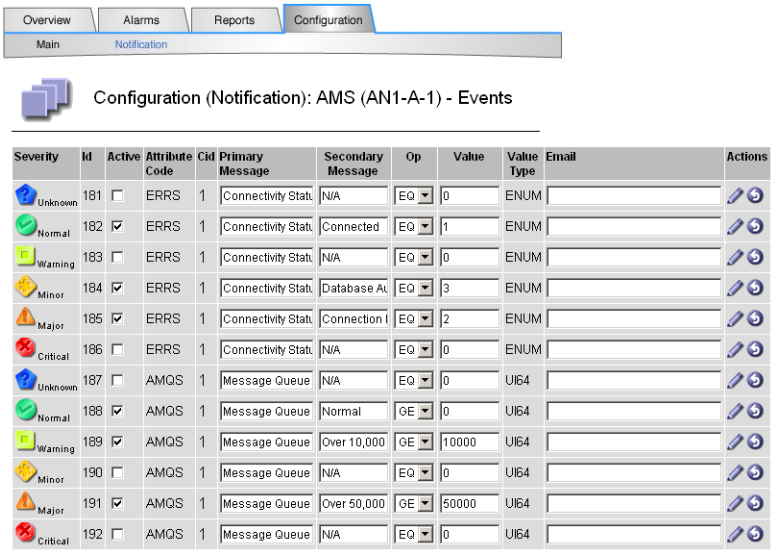
For general information about alarm concepts, levels, and handling consult Chapter 3: “Alarms” on page 25.

Configuration—Notification Page

The Configuration ▶ Notification page enables you to:

- Select which attributes the NMS monitors for an alarm state
- Set the specific parameters for each alarm level

The attribute data is presented in a detailed table with each alarm level listed for every attribute that can be monitored.



Severity	Id	Active	Attribute Code	Cid	Primary Message	Secondary Message	Op	Value	Value Type	Email	Actions
Unknown	181	☐	ERRS	1	Connectivity Statu	N/A	EQ	0	ENUM		
Normal	182	☑	ERRS	1	Connectivity Statu	Connected	EQ	1	ENUM		
Warning	183	☐	ERRS	1	Connectivity Statu	N/A	EQ	0	ENUM		
Minor	184	☑	ERRS	1	Connectivity Statu	Database Au	EQ	3	ENUM		
Major	185	☑	ERRS	1	Connectivity Statu	Connection I	EQ	2	ENUM		
Critical	186	☐	ERRS	1	Connectivity Statu	N/A	EQ	0	ENUM		
Unknown	187	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		
Normal	188	☑	AMQS	1	Message Queue	Normal	GE	0	UI64		
Warning	189	☑	AMQS	1	Message Queue	Over 10,000	GE	10000	UI64		
Minor	190	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		
Major	191	☑	AMQS	1	Message Queue	Over 50,000	GE	50000	UI64		
Critical	192	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		

Figure 27: Sample Notification Configuration Table

You can configure five fields within the Notification table (indicated with the icon in the following table):

Table 59: Notification Table Headings

Heading	Description
Severity	The icon and text indicating the level of the alarm (see "Alarm Levels and Indicators" on page 28).
Id	A unique number (within the entire grid) allocated to the alarm, level, and service/ component.
Active	A check box to enable or disable the attribute alarm monitoring for the particular level.
Attribute Code	The system code for the attribute being monitored. This code is used to lookup alarms in the chapter "Troubleshooting Alarms" on page 171.
CId	A sequence number to identify alarm sources that are listed as rows in a table (such as VMFR in the SSM ▶ Volumes component). The number indicates the table row, counting from the top.
Primary Message	Describes the function of the attribute being monitored.
Secondary Message	Details the reason for the alarm (connection lost, storage space below 10%, and so on)
Op	A pull-down menu of operators. Select the one for testing the current attribute value against the Value threshold: • EQ—equals (=) • GE—greater than or equal to (>=) • LE—less than or equal to (<=) • NE—not equal to (!=) When the operation "*attrval* Op Value" evaluates "true", the alarm is set to that level. See Figure 15: "Alarm Monitoring Algorithm" on page 27 for more details.

Table 59: Notification Table Headings (cont.)

Heading	Description
Value	The alarm's threshold value used to test (using Op) against the attribute's actual value.
Value Type	An indication of the data type of the attribute: • UI32—Unsigned Integer, 32-bit • UI64—Unsigned Integer, 64-bit • SI64—Signed Integer, 64-bit • ENUM—Enumerated Integer • CSTR—"C"-style String • SF64—Signed Floating-point, 64-bit • UF32—Unsigned Floating-point, 32-bit
Email	Not used by the HP Medical Archive.
Actions	Control buttons to: Write (apply) the setting Undo—revert to the last applied setting

Active Alarms

When the Active check box is selected, the attribute status is monitored on the Status page and an alarm status icon appears beside the attribute's name on the Overview page. If the attribute's value reaches the configured alarm threshold, the contact specified in the Email column is alerted.

The figures on the next page show an example of fields selected on the Configuration ▶ Notification page. Attribute alarms selected as Active on the Notification page (Figure 28) display alarm icons in the appropriate attribute row under the Overview tab (Figure 29).

Overview | Alarms | Reports | Configuration

Main | Notification

Configuration (Notification): AMS (AN1-A-1) - Events

Severity	Id	Active	Attribute Code	Cid	Primary Message	Secondary Message	Op	Value	Value Type	Email	Actions
Unknown	181	☐	ERRS	1	Connectivity Statu	N/A	EQ	0	ENUM		
Normal	182	☑	ERRS	1	Connectivity Statu	Connected	EQ	1	ENUM		
Warning	183	☐	ERRS	1	Connectivity Statu	N/A	EQ	0	ENUM		
Minor	184	☑	ERRS	1	Connectivity Statu	Database Au	EQ	3	ENUM		
Major	185	☑	ERRS	1	Connectivity Statu	Connection I	EQ	2	ENUM		
Critical	186	☐	ERRS	1	Connectivity Statu	N/A	EQ	0	ENUM		
Unknown	187	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		
Normal	188	☑	AMQS	1	Message Queue	Normal	GE	0	UI64		
Warning	189	☑	AMQS	1	Message Queue	Over 10,000	GE	10000	UI64		
Minor	190	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		
Major	191	☑	AMQS	1	Message Queue	Over 50,000	GE	50000	UI64		
Critical	192	☐	AMQS	1	Message Queue	N/A	EQ	0	UI64		

Figure 28: Sample Alarm Settings

Overview | Alarms | Reports | Configuration

Main

Overview: AMS (AN1-A-1) - Events

Updated: 2005-01-14 at 16:19:17 PST

Connectivity Status:	Connected to Database
Audit Messages Received:	6,902,804 Msgs
Audit Message Receive Rate:	0.83 Msgs/s
Audit Messages Queued:	6,516,663 Msgs
Audit Message Commit Rate:	9.50 Msgs/s
Audit Messages Committed:	386,140 Msgs

ERRS

AMQS

Figure 29: Sample Alarm Icons in Overview

You can see the indicator on the default (Overview) page and click the alarm indicator to jump to the status information.

Changing Alarm Settings

All notification settings are managed in the same manner. Settings are considered permanent until explicitly altered; they are retained when the service is restarted.

CAUTION

Alarm settings are enabled as part of your grid installation. Changes to alarm settings should not be made for simple convenience; this may conceal underlying problems that should be resolved. If you find an alarm is persistent, discuss the situation with HP technical support before making changes.

Enabling (or Disabling) an Alarm

To activate (or disable) monitoring for an alarm:

1. Locate the row for the desired attribute and alarm level you wish to configure.
2. Enable (or deselect) the **Active** check box in that row.
3. Click the Write button in the Actions column to apply the setting.

Setting an Alarm Threshold

To customize an alarm's threshold value:

1. Locate the row for the desired attribute and alarm level you wish to configure.
2. Ensure the **Active** check box in that row is enabled.
3. Enter an appropriate **Secondary Message** describing the condition.
4. Use the **Op** pull-down menu to select the desired comparison operation (*attrval* Op Value).
5. Set the threshold **Value** for the comparison operation.
6. Click the Write button in the Actions column to apply the setting.

Service and Component Configuration

WARNING

Changing configuration settings requires careful and deliberate planning. Some configurable elements can affect the state of your live system. Only experienced administrators should alter the device and component configuration settings.

Configuration—Main Page

The Configuration Main page of each service provides a form to customize labels, add notes, and other features.

Configuration changes entered in the form are not made until you select the Apply *button (bottom right corner of the page). Changes made to the configuration settings may take time to process. Do* not *click the* Apply *button more than once. Wait for your browser to refresh the page.*

The full set of available settings on the Configuration Main page depend on the service or component being configured. Some values of enumerated attribute types may not be available for user setting. The following sections outline the specific settings for each service and its associated components. The settings common to all services are described here.

Table 60: Main Page Configuration Settings Common to All Services

Prompt	Type	Description
State	Pull-down menu	Sets the service to be either: • Online—normal operation, providing service to the grid. • Standby (only available on CLB)—halts service to the grid but maintains a grid connection.
User Label	String	This string is the identification tag that appears in the Navigation Tree, map views, and as the heading in the Content frame for the service on this node.

Table 60: Main Page Configuration Settings Common to All Services (cont.)

Prompt	Type	Description
Notes	Text	Free form notes allowing you to add descriptive text related to the service on this node. These notes appear in the Node Information section of the Overview page.

The NMS categorizes system information by the services and service components found on each node. These services and components may contain configurable settings. This chapter provides a complete list of services and their related components. Services are listed alphabetically.

Not all grids use every service and component listed here. Each grid uses only those services and components suited to the options purchased and the functionality required.

Within a grid, the same service can be installed and used on more than one node. The settings made to a service on one node do *not* affect the settings on the same service installed on a different node.

The Configuration Management Node (CMN) service is used to make configuration settings on a system-wide basis, for protocol handling and network permissions. Access to these settings is restricted to the Vendor account. Details are not included in this guide.

ADC Configuration

The Administrative Domain Controller (ADC) Configuration ▶ Main page offers the standard service settings to change the labeling of the service and add notations, see Table 60 on page 158.

ADC Components

The only component supported by the ADC is the Connectivity component, which does not have configurable settings.

AMS Configuration

The Audit Management System (AMS) supports the standard service settings to change the labeling of the service and add notations, see Table 60 on page 158.

AMS Components

In addition to the standard service settings, the AMS also supports the following components:

- Events
- Connectivity

There are no configurable settings offered for these components.

CLB Configuration

The Connection Load Balancer (CLB) offers the standard service settings to change the labeling of the service and add notations, see Table 60 on page 158.

CLB Components

The CLB supports the following components:

- DICOM
- HTTP
- Connectivity

DICOM

DICOM is optional on the HPMA.

This component provides a check box to reset the DICOM event counters. This can be used to clear alarm conditions.

Table 61: CLB ▶ DICOM Component Configuration Settings

Prompt	Type	Description
Reset DICOM Counts	Check box	When selected and applied, all counter attributes of the CLB DICOM incoming and outgoing associations are reset to zero.

HTTP

This component provides a check box to reset the HTTP event counters. This can be used to clear alarm conditions.

Table 62: CLB ▶ DICOM Component Configuration Settings

Prompt	Type	Description
Reset HTTP Counts	Check box	When selected and applied, all counter attributes of the CLB HTTP sessions are reset to zero.

Connectivity

There are no configurable settings offered for this component.

CMN Configuration

The CMN Configuration ▶ Main page offers the standard service settings to change the labeling of the service and add notations, see Table 60 on page 158.

The Configuration Management Node (CMN) service is used to make configuration settings on a system-wide basis, for protocol handling and network permissions. Access to the settings for components of this service is restricted to the Vendor account. Details are not included in this guide.

CMS Configuration

The Content Management System (CMS) manages content according to business rules configured to replicate content in the most robust manner available in your grid deployment.

The CMS manages access to the grid's data. It also supports queries related to content metadata.

The CMS supports the standard service settings to change the labeling of the service and add notations, see Table 60 on page 158.

CMS Components

The CMS also supports the following components:

- Content
- Database
- DICOM
- Synchronization
- Connectivity

There are no configurable settings offered for these components.

FSG Configuration

The File System Gateway (FSG) supports the standard service settings to change the labeling of the service and add notations, see Table 60 on page 158.

FSG Components

In addition to the standard service settings, the FSG also supports the following components:

- Storage
- Replication
- Backup
- Client Services
- Connectivity

Only the Storage component offers configurable settings.

Storage

This component provides check boxes to reset event counters. This can be used to clear alarm conditions.

Table 63: FSG ▶ Storage Component Configuration Settings

Prompt	Type	Description
Reset Retrieve from Grid Failure Count	Check box	When selected and applied, the counter attribute for "Files Retrieved from Grid - Failed" is reset to zero. This clears the "FRGF" alarm.
Reset Validation Failure Counts	Check box	When selected and applied, the counter attribute for "Part 10 Validation Failures" is reset to zero. This clears the "FDPP" alarm. This only applies if the DICOM option is installed.

LDR Configuration

The Local Distribution Router (LDR) supports the standard service settings to change the labeling of the service and add notations. It also offers settings to control the state of the storage and protocol components. The full set of configurable settings is shown below.

Table 64: LDR Service Configuration Settings

Prompt	Type	Description
LDR State	Pull-down menu	Sets the service state: • Online—normal operation
Storage State	Pull-down menu	This is a duplicate of the setting on the component's main configuration settings. See page 165.
DICOM State	Pull-down menu	This is a duplicate of the setting on the component's main configuration settings. See page 166.
HTTP State	Pull-down menu	This is a duplicate of the setting on the component's main configuration settings. See page 167.
User Label	String	This string is the identification tag that appears in the Navigation Tree, map views, and as the heading in the Content frame for this service on this node.
Notes	Text	Free form notes allowing you to add descriptive text related to this service on this node. These notes appear in the Node Information section of the Overview page.

LDR Components

In addition to the standard service settings, the LDR also supports the following components:

- Storage
- DICOM
- HTTP
- Connectivity

Storage

This component provides data on the object storage space and the objects processed. The Storage component tracks the total amount of object storage space being used and the space available.

The configuration settings allow you to set the active state of the storage component, force the storage to read-only on restart, and reset the "OCOR" alarm.

Table 65: LDR ▶ Storage Component Configuration Settings

Prompt	Type	Description
Storage State	Pull-down menu	Sets the component to be: • Standby— When Storage is taken offline (standby), the DICOM and HTTP interfaces are forced into Redirect state and no replications are made to or from the storage node. • Online (Read-Only)—tells the grid this service is not accepting new content. If DICOM or HTTP components are Online, they are forced to Online (Read-Only) state. • Online—normal operation
Storage Read-Only on Startup	Check box	Sets the storage component to be read-only when the component is restarted. Otherwise the state is set by the service based on the available object storage space. If space is low, the component uses Online (Read-Only), otherwise it is Online. You can use this setting to force the storage to read-only even when there is ample available space. This can be useful for troubleshooting.
Reset Corrupt Objects Count	Check box	When selected and applied, the counter attribute for "Corrupt Objects Detected" is reset to zero. This clears the "OCOR" alarm.

DICOM

DICOM is optional on the HPMA.

The configuration settings for the LDR ▶ DICOM component allow you to set the active state of the protocol component, select whether or not to enable the protocol on service restarts, and reset transaction counters to clear alarms.

The LDR advertises two ports to the grid, one for query and retrieve operations and one for ingest. When the DICOM component is in "Online" state, both ports are advertised. The "Online (Read-Only)" state advertises only the Q/R port and not the ingest port.

Table 66: LDR ▶ DICOM Component Configuration Settings

Prompt	Type	Description
DICOM State	Pull-down menu	Sets the component to be either: • Offline—No DICOM transactions are allowed, and any entity that tries to establish a DICOM association to the LDR receives an error message. Active associations are completed normally. DICOM component counter attributes are reset to zero. • Redirect—Transparently redirects associations to other LDR services. No DICOM processing is performed locally. • Online (Read-Only)—Only the Q/R DICOM port is advertised to the grid. • Online—Normal operation.
Auto-Start DICOM	Check box	Enables the DICOM component when the service is restarted. If not selected, the DICOM component remains Offline until explicitly enabled. If the check box is selected, the state on restart depends on the state of the Storage component. If the storage component is read-only on startup, the DICOM interface is also read-only. If the storage component is online, then DICOM is also online. Otherwise the DICOM interface remains in the Offline state.
Reset DICOM Counts	Check box	When selected and applied, the counter attributes for DICOM transactions are reset to zero. This can be used to clear alarms.

HTTP

The configuration settings for the LDR ▶ HTTP component allow you to set the basic state of the protocol component, select whether or not to enable the protocol on service restarts, and reset transaction counters to clear alarms.

Table 67: LDR ▶ HTTP Component Configuration Settings

Prompt	Type	Description
HTTP State	Pull-down menu	Sets the component to be either: • Offline—No HTTP transactions are allowed, and any user who tries to open an HTTP session to the LDR receives an error message. Active sessions are gracefully closed. HTTP component counter attributes are reset to zero. • Redirect—Transparently redirects sessions to other LDR services. No HTTP processing is performed locally. • Online (Read-Only)—Only query and retrieve operations are permitted. • Online—Normal operation.
Auto-Start HTTP	Check box	Enables the HTTP component when the service is restarted. If not selected, the HTTP interface remains Offline until explicitly enabled. If the check box is selected, the state on restart depends on the state of the Storage component. If the storage component is read-only on startup, the HTTP interface is also read-only. If the storage component is online, then HTTP is also online. Otherwise the HTTP interface remains in the Offline state.
Reset HTTP Counts	Check box	When selected and applied, the counter attributes for HTTP transactions are reset to zero. This can be used to clear alarms.

Connectivity

There are no configurable settings offered for the Connectivity component.

NMS Configuration

The Network Management System supports the standard service settings to change the labeling of the service and add notations, see Table 60 on page 158.

NMS Components

In addition to the standard service settings, the NMS also supports the following components:

- Database
- Connectivity

There are no configurable settings offered for these components.

SSM Configuration

The Server Status Monitor (SSM) supports the standard service settings to change the labeling of the service and add notations, see Table 60 on page 158.

SSM Components

In addition to the standard service settings, the SSM also supports the following components:

- Events
- Volumes
- RAID
- Services
- Network

Events

The Events component provides counters for a variety of errors. The configuration page enables you to reset the counter to zero (0) for any selected event types.

Table 68: SSM ▶ Events Component Configuration Settings

Prompt	Type	Description
Description	Text	Identifies the event being reported. (Display only; cannot be configured.)
Count	Text	Indicates the current counter value for the event type. (Display only; cannot be configured.)
Reset	Check box	Enables resetting the counter to zero (0).

The selected counters are only reset when the Apply button is selected.

To reset error event counters:

1. Select the **SSM ▶ Events** component in the Navigation Tree.
2. Select the **Configuration ▶ Main** page.
3. Select the **Reset** column check boxes for specific event counters to be reset.
4. Click the **Apply** button to reset the checked counters.

Volumes

There are no configurable settings offered for the Volumes component.

RAID

There are no configurable settings offered for the RAID component.

Services

There are no configurable settings offered for the Services component.

Network

The Network component of the SSM service is distinct from other services. The SSM ▶ Network ▶ Configuration ▶ Main page provides the ability to reset the error counters.

Table 69: SSM ▶ Network Component Configuration Settings

Prompt	Type	Description
Clear Error Counts	Check box	Resets all network component error and fault counters. This clears the “FERR” alarm.
Devices		
Name	Display only	Operating system name for the physical network port.
Label	Text	User-defined label for the port.
IP Address	Display only	Address assigned to the port at installation.

Troubleshooting Alarms

7

Chapter Contents

Overview 172
Alarm Reference Table 172

HP Medical Archive

Overview

Troubleshooting consists primarily of how to respond to various alarms. This chapter provides a detailed table with the alarm codes and the suggested response. If a serious issue arises to which no answer is provided in this chapter, contact HP technical support directly.

Alarm Reference Table

The NMS comes with a series of pre-configured alarms when the system is implemented. Each alarm can be configured to suit your grid management needs. Responses are assigned according to the severity of the alarm. This may vary if you customize the alarm settings to fit your system management approach.

Attr. Code	Description	Recommended Action
ADCA	ADC Device Status; indicates the general status of the ADC service: • 0 = No errors • 10 = Errors	If there is an Error, check the Overview and Alarm tabs for the device to find the cause of the error and to troubleshoot the problem. If the problem persists, contact HP technical support.
ADCE	ADC Device State; whether the device is: • 0 = Offline • 1 = Standby • 2 = Online	If the device goes into “Standby”, continue monitoring and if the problem persists, contact HP technical support. If the device goes into “Offline” and there are no known server hardware issues (server unplugged) or a scheduled downtime for the device, contact HP technical support.

Attr. Code	Description	Recommended Action
AMQS	Audit Message Queue Size; a count of audit messages waiting in the queue to be committed to the database. Alarms are based on the queue being over a specified threshold. During heavy loads the queue can go over 10,000 or even 50,000, but at that level it should be closely monitored.	Check the load on the system—if there have been a significant number of transactions this may be normal and will resolve itself over time. If the alarm persists, view a chart of the queue size. If the number continues increasing without ever decreasing, contact HP technical support.
AUMA	AMS Device Status; indicates the general status of the AMS service: • 0 = No errors • 1 = DB Connectivity Error	If the service indicates "DB Connectivity Error", restart the server. If this does not clear the problem, contact HP technical support.
AUME	AMS Device State; whether the device is: • 0 = Offline • 1 = Standby • 2 = Online	If the device goes into "Standby", continue monitoring and if the problem persists, contact HP technical support. If the device goes into "Offline" and there are no known server hardware issues (server unplugged) or a scheduled downtime for the device, contact HP technical support.
CAID	Count of Available Ingest Destinations; nodes that accept connections for ingesting content. Normally there is more than one in a grid. When there is only one, a warning is set; having none is a major alarm condition.	This alarms clear when underlying issues of available LDR services are corrected. Ensure the DICOM (for CAID/CAQD) and HTTP (for CAIH/CAQH) components of LDRs are online and running normally.
CAIH		
CAQD	Count of Available Q/R Destinations; nodes accepting connections for content query and retrieve operations. Normally there is more than one in a grid. When there is only one, a warning is set; having none is a major alarm condition.	
CAQH		

Attr. Code	Description	Recommended Action
CIAF	Count of Incoming Associations Failed; the number of DICOM associations that failed to connect at the TCP/IP layer. More than 50 is considered a minor alarm to investigate further.	Failures could be caused by either end of the association. Check the CLB ▶ DICOM component to determine if the failures are client side or node side. Client side faults indicate a problem with the remote entity. If consistent faults appear on the node side, contact HP technical support.
CISF	Count of Incoming HTTP Sessions Failed; the number of HTTP session requests that failed to connect at the TCP/IP layer. More than 50 is considered a minor alarm to investigate further.	Failures could be caused by either end of the association. Check the CLB ▶ HTTP component to determine if the failures are client side or node side. Client side faults indicate a problem with the remote entity. If consistent faults appear on the node side, contact HP technical support.
CLBA	CLB Device Status; indicates the general status of the CLB service: • 0 = No errors • 10 = Errors	If there is an Error, check the Overview and Alarm tabs for the device to find the cause of the error and to troubleshoot the problem. If the problem persists, contact HP technical support.
CLBE	CLB Device State; whether the device is: • 0 = Offline • 1 = Standby • 2 = Online	If the device goes into “Standby”, continue monitoring and if the problem persists, contact HP technical support. If the device goes into “Offline” and there are no known server hardware issues (server unplugged) or a scheduled downtime for the device, contact HP technical support.

Attr. Code	Description	Recommended Action
CMNA	CMN Device Status; indicates the general status of the CMN service: • 0 = No errors • 10 = Errors	If there is an Error, check the Overview and Alarm tabs for the device to find the cause of the error and to troubleshoot the problem. If the problem persists, contact HP technical support.
CMNE	CMN Device State; whether the device is: • 0 = Offline • 1 = Standby • 2 = Online	If the device goes into "Standby", continue monitoring and if the problem persists, contact HP technical support. If the device goes into "Offline" and there are no known server hardware issues (server unplugged) or a scheduled downtime for the device, contact HP technical support.
COAF	Count of Outgoing Associations Failed; the number of DICOM associations that failed to connect at the TCP/IP layer. More than 50 is considered a minor alarm to investigate further.	Failures could be caused by either end of the association. Check the CLB ▶ DICOM component to determine if the failures are client side or node side. Client side faults indicate a problem with the remote entity. If consistent faults appear on the node side, contact HP technical support.
CsQL	Estimated count of incoming CMS Synchronization messages that must be processed. More than 50,000 is considered a minor alarm to investigate further. More than 1,000,000 is considered a critical condition.	Check the load on the system—if there have been a significant number of transactions this may be normal and will resolve itself over time. If the alarm persists, view a chart of the queue size. If the number continues increasing without ever decreasing, contact HP technical support.

Attr. Code	Description	Recommended Action
CsQT	Count of CMS Synchronization messages that are queued to be sent to other CMS services. More than 50,000 is considered a minor alarm to investigate further. More than 1,000,000 is considered a critical condition.	Ensure that other CMS services are online and running normally. Check the load on the system—if there have been a significant number of transactions this may be normal and will resolve itself over time. If the alarm persists, view a chart of the queue size. If the number continues increasing without ever decreasing, contact HP technical support.
DBSF	Remaining Database Space; the number of bytes remaining in the allocated database for CMS metadata. Adjusting the alarm threshold allows you to proactively manage when additional storage needs to be allocated.	If the available space is reaching a low threshold, you should contact HP technical support to arrange for the database allocation to be enlarged.
DCiN	Number of unprocessed new content objects. More than 1000 is considered cause for investigation.	If the number persists for some time after new content has been stored, contact HP technical support.

Attr. Code	Description	Recommended Action
DEAE	Count of inbound DICOM C-Echo failures. 50 is considered a minor issue.	These alarms indicate a problem with executing specific activities in the DICOM protocol. Check the log at the remote entity to determine if the errors are originating with the modality or the grid. If the modality shows the errors, then adjust the configuration of the entity. If the errors are on the grid side of the connection, contact HP technical support. To reset the counters, use the Configuration ▶ Main page; see "DICOM" on page 166.
DEAF	Count of inbound DICOM C-Find failures. 50 is considered a minor issue.	
DEAI	Count of inbound DICOM C-Store failures. 50 is considered a minor issue.	
DEAM	Count of inbound DICOM C-Move failures. 50 is considered a minor issue.	
DEAO	Count of outbound DICOM C-Store failures. 50 is considered a minor issue.	
DEEO	Count of outbound DICOM C-Echo failures. 50 is considered a minor issue.	
DEIA	Count of inbound DICOM association failures from external sources (after the TCP/IP layer). 50 is considered a minor issue.	
DEOA	Count of outbound DICOM association failures to external destinations (after the TCP/IP layer). 50 is considered a minor issue.	
DESC	Count of inbound Storage Commitment failures. 50 is considered a minor issue.	

Attr. Code	Description	Recommended Action
DSN*n*	HD Status; the status of each of the drives in a RAID unit: • 0 = No Errors • 1 = Rebuilding • 2 = Missing • 3 = Unknown • 4 = Failed • 5 = Spare • 6 = Replaced The letter *n* in the Attribute Code is an indicator of which RAID, as some servers are attached to multiple RAID units. All the drives are assigned to their respective array utilizing the Cid to distinguish each individual drive.	Should a drive indicate "Missing", "Failed", or "Unknown", check the physical hardware and resolve any hardware issues. Often the drive needs to be replaced with a spare.
ERRS	Connectivity Status; between the AMS and its database. • 0 = Connecting to Database • 1 = Connected to Database • 2 = Connectivity to Database Lost, Reconnecting • 3 = Database Authentication Failed, Retrying Not used in the HP Medical Archive.	This alarm indicates an installation problem. Contact HP technical support.
FCSA	FSG Client Services component Status; indicates: • 0 = No errors • 10 = Client Service Error A "Client Service Error" indicates a problem with CIFS or NFS export functionality.	Restart the service. If the problem persists, contact HP technical support.
FDPP	Not used by the HP Medical Archive.	N/A

Attr. Code	Description	Recommended Action
FERR	Sum of all errors reported by a network interface port. At 50, monitoring the situation is advised. At 100, a minor issue investigation is needed. At 500, the issue is considered major.	Check that the adapter hardware and driver are correctly installed and configured to work with your network routers and switches. When the underlying problem is resolved, use the Configuration tab to clear the alarm. See page 170.
FGWA	FSG Device Status; indicates the general status of the FSG service: • 0 = No errors • 1 = Waiting for CMSs • 2 = Starting • 3 = Shutting Down FSG devices need to be connected to at least one CMS to process transactions.	If the service indicates "Waiting for CMSs", ensure at least one CMS is online and running without errors.
FGWE	FSG Device State; whether the device is: • 0 = Offline • 1 = Standby • 2 = Online	If the device goes into "Standby", continue monitoring and if the problem persists, contact HP technical support. If the device goes into "Offline" and there are no known server hardware issues (server unplugged) or a scheduled downtime for the device, contact HP technical support.
FOPN	Open file descriptors. A measure of operating system resource use. This value should fluctuate as files are opened and closed. 800 is considered an unusually high number.	This value can become large during peak activity. If it does not diminish during periods of slow activity, contact HP technical support.

Attr. Code	Description	Recommended Action
FRGF	Files Retrieved from the Grid (Failed); a count of files requested through an FSG but have failed to be retrieved from the grid to the cache. Values of fifty or more are a minor concern.	Ensure all CMS and LDR nodes are operating normally. If the value continues to increase, contact HP technical support. When the underlying problem is resolved, use the Configuration tab to clear the alarm. See page 163.
FRGP	Files Retrieved from the Grid (Pending); a count of files requested through an FSG but not yet retrieved from the grid to the cache. Requests are arriving faster than the grid can respond. Values of 20 or more are a minor concern.	Ensure all CMS and LDR nodes are operating normally. Reduce demand on the grid if possible. If the problem persists, contact HP technical support.
FRGR	Files Retrieved from the Grid (Retrying); a count of files requested through an FSG but have failed to be retrieved from the grid to the cache and are being retried. Values of five or more are a minor concern.	Monitor the situation. If the values do not decrease, contact HP technical support.
FSGP	Files Stored to Grid (Pending); a count of files cached to an FSG but not yet confirmed as ingested to the grid. Objects are arriving faster than the grid can manage. Values of 2000 or more are a major concern.	Ensure all CMS and LDR nodes are operating normally. Reduce ingests to the grid if possible. If the problem persists, contact HP technical support.
FSGR	Files Stored to Grid (Retrying); a count of files cached to an FSG but have failed to be ingested to the grid and are being retried. Values of five or more are a minor concern.	Monitor the situation. If the values do not decrease, contact HP technical support.

Attr. Code	Description	Recommended Action
FSTA	FSG Total Available cache; a measure of remaining space on the server for caching content. Cache space is managed by the service. Space is freed as objects in the cache are no longer needed. Values less than 30 GB trigger alarms.	Ensure all CMS and LDR nodes are operating normally. Check the following attributes in the FSG ▶ Storage component: "Files Stored to Grid - Pending", "File Store Rate", and "File Retrieved Rate". If these measures of cache activity are high, attempt to reduce demand until the alarm clears. If the problem persists, contact HP technical support.
HEID	Count of inbound HTTP DELETE failures. 50 is considered a minor issue.	These alarms indicate a problem with executing specific activities in the HTTP protocol. Check the log at the remote entity to determine if the errors are originating with the remote workstation (entity) or the grid. If the entity shows the errors, then adjust the configuration of the entity. If the errors are on the grid side of the connection, contact HP technical support. *Note: Deleting or renaming files recently stored to the FSG can produce this alarm if the FSG was actively relaying the file to the grid. Reset the counter.* To reset the counters, use the Configuration ▶ Main page; see "HTTP" on page 167.
HEIG	Count of inbound HTTP GET failures. 50 is considered a minor issue.	
HEIH	Count of inbound HTTP HEAD failures. 50 is considered a minor issue.	
HEIO	Count of inbound HTTP OPTION failures. 50 is considered a minor issue.	
HEIP	Count of inbound HTTP PUT failures. 50 is considered a minor issue.	
HEIS	Count of inbound HTTP Session negotiation failures (after the TCP/IP layer). 50 is considered a minor issue.	
HEIT	Count of inbound HTTP POST failures. 50 is considered a minor issue.	

Attr. Code	Description	Recommended Action
HSTE	HTTP State; protocol component state: • 0 = Offline • 1 = Redirect • 2 = Online (Read-only) • 3 = Online If you are using the FSG service, it is critical that the HTTP protocol be online and running without errors.	Check the state of the LDR and the related Storage component. Ensure all are online. Check that the HTTP component is configured to autostart when the service is restarted (page 167).
HSTU	HTTP Status; protocol component status: • 0 = No Errors • 2 = Not Started • 3 = Starting... • 4 = Stopping...	
LDRA	LDR Device Status; indicates the general status of the LDR service: • 0 = No errors • 1 = Waiting for CMSs • 2 = Shutting Down LDR devices need to be connected to at least one CMS to process transactions.	If the service indicates “Waiting for CMSs”, ensure all CMS nodes are operating normally. If problems persist, contact HP technical support.
LDRE	LDR Device State; whether the device is: • 0 = Offline • 1 = Standby • 2 = Online	If the device goes into “Standby”, continue monitoring and if the problem persists, contact HP technical support. If the device goes into “Offline” and there are no known server hardware issues (server unplugged) or a scheduled downtime for the device, contact HP technical support.
MSTE	State of the DICOM protocol component: • 0 = Offline • 1 = Redirect • 2 = Online (Read-only) • 3 = Online	Check the state of the LDR and the related Storage component. Ensure all are online. Check that the DICOM component is configured to autostart when the service is restarted (page 166).

Attr. Code	Description	Recommended Action
MSTU	Status of the DICOM protocol component: • 0 = No Errors • 1 = Not Started • 2 = Invalid/Missing DICOM Dictionary • 3 = Starting... • 4 = Stopping... • 5 = Invalid/Missing Index Tag List	Restart the service. If the error persists, it may indicate an installation problem. Contact HP technical support.
NADC	Number of ADCs the device is connected to. There should always be at least one ADC. If there are no connected ADCs, the server starts drifting in relative time, which may affect system operations and synchronization over longer periods.	Restore connectivity to an ADC as soon as possible. This may require updating authentication certificates. If this condition persists, contact HP technical support.
NAMS	Number of AMSs the device is connected to. If there are no connected AMSs, the device cannot report audit events and they are queued and unavailable to users until the AMS connection is restored.	Restore connectivity to an AMS as soon as possible. This may require updating authentication certificates. If this condition persists, contact HP technical support.
NANG	Network Auto Negotiate setting: • 0 = Off • 1 = On • 2 = Unavailable • 3 = Unknown • 4 = Unsupported	Check the network adapter configuration. The setting must match preferences of your network routers and switches. An incorrect setting can have a severe impact on grid performance.

Attr. Code	Description	Recommended Action
NCMS	Number of CMSs the device is connected to. The system needs multiple CMSs to maintain fault tolerance and quality of service. If there is no connected CMS under LDR ▶ Network, there are no CMSs available and end user functionality may be impacted. If there is no connected CMS under CMS ▶ Network, there is at least one CMS running (itself) and system operation is not impacted.	Restore connectivity to a CMS as soon as possible. This may require updating authentication certificates. If the condition persists, contact HP technical support.
NDBC	NMS Database component Connectivity status: • 0 = Connecting... • 1 = Connected • 2 = Connection Lost, Reconnecting... • 3 = Connection Timeout, Retrying... • 4 = Authentication Failed, Retrying...	If the service indicates "Authentication Failed, Retrying...", restart the service. If the problem persists, contact HP technical support.
NDUP	Network Duplex setting: • 0 = Full • 1 = Half • 2 = Unavailable • 3 = Unknown • 4 = Unsupported	Check the network adapter configuration. The setting must match preferences of your network routers and switches. An incorrect setting can have a severe impact on grid performance.
NLNK	Network Link Detect: • 0 = Down • 1 = Up • 2 = Unavailable • 3 = Unknown • 4 = Unsupported	Check the network cable connections on the port and at the switch. Check the network router, switch, and adapter configurations. Restart the server. If the problem persists, contact HP technical support.

Attr. Code	Description	Recommended Action
NNMS	Number of NMSs the device is connected to. Connections to the NMS do not affect client functionality, but do affect your ability to properly monitor the system.	If there is no connection to an NMS, check the network connections and whether both servers and services are available. If this is not a hardware related issue and the problem persists, contact HP technical support.
NSCA	NMS Device Status; indicates the general status of the NMS service: • 0 = No errors • 1 = DB Connectivity Error	If the service indicates "DB Connectivity Error", restart the service. If the problem persists, contact HP technical support.
NSCE	NMS Device State; whether the device is: • 0 = Offline • 1 = Standby • 2 = Online	If the device goes into "Standby", continue monitoring and if the problem persists, contact HP technical support. If the device goes into "Offline" and there are no known server hardware issues (server unplugged) or a scheduled downtime for the device, contact HP technical support.
NTBR	Remaining Database Space; the number of bytes remaining in the allocated database for NMS attribute data. Adjusting the alarm threshold allows you to proactively manage when additional storage needs to be allocated.	If the available space is reaching a low threshold, you should contact HP technical support to arrange for the database allocation to be enlarged.
OCOR	Objects Corrupt; the number of objects stored on this LDR that have been detected as potentially corrupt and need to be investigated. Any corrupt objects are worthy of investigation. More than 10 indicates a critical problem.	If there are several corrupt objects identified, contact HP technical support. After the underlying problem is resolved, use the Configuration tab to clear the alarm. See page 165.

Attr. Code	Description	Recommended Action
PAT*n*	RAID controller status; indicates the status of the RAID *monitoring* and is not an indicator of the status of the RAID itself: • 0 = Online • 1 = Offline The letter *n* in the Attribute Code is an indicator of which RAID, as some servers are attached to multiple RAID units. The monitoring module is used to report statistics on the RAID.	Under certain circumstances the monitoring module can become shut down or disconnected. Once it is brought back up, it initializes and rebuilds the array if necessary, then goes into "Online" state again. Check the RAID monitoring serial cable at the back of the server to make sure it is connected properly. If this problem persists for a period of time, unplug the serial cable from the back and plug it back in. If the RAID monitoring still does not initialize, contact HP technical support.
PBST	FSG Backup result; whether the backup was: • 0 = Successful • 1 = Failed	If the backup reports "Failed", ensure there are no coincident HTTP alarms on LDR nodes and that capacity remains on some Storage Nodes. Backups are run automatically each day, and retained for two weeks.
PFA*n*	Fan State; indicates the state of the internal fan for the RAID: • 0 = OK • 1 = Speed Low • 2 = Speed High • 3 = Stopped • 4 = Failed • 5 = Unavailable The letter *n* in the Attribute Code is an indicator of which RAID, as some servers are attached to multiple RAID units.	If the fan state is anything other than "OK" (0), check the fan in the unit to ensure proper operation. If it is functioning properly but this alarm persists, contact HP technical support.

Attr. Code	Description	Recommended Action
PMEM	Memory Usage (%); the percentage of RAM memory that is being used. Can have values "Over *Y*% RAM" where *Y* represents the percentage of memory being used by the server. Figures under 70% are normal. Over 95% is considered a major issue.	If the memory usage is fairly high for a single device/service, this should be monitored and investigated. Should it reach over 99% RAM and this alarm continues to persist, contact HP technical support.
PPS*n*	Power Supply Status; an overall indication of whether the RAID array's power supply is functional: • 0 = No Errors • 1 = VRM Removed • 2 = VRM Failed • 3 = Power Supply Fault • 4 = Unavailable The letter *n* in the Attribute Code is an indicator of which RAID, as some servers are attached to multiple RAID units.	If the RAID array is "VRM Removed", "VRM Failed", or "Power Supply Fault", check the power supply hardware for the RAID array unit. If this does not appear to be a hardware problem, contact HP technical support.
PSA*n*	Array State: • 0 = Online • 1 = Offline The letter *n* in the Attribute Code is an indicator of which Array, as some servers are attached to multiple arrays.	If the array is offline, check the physical hardware to make sure it is alright and that it is cabled correctly. If this does not appear to be a hardware problem, contact HP technical support.
PSN*n*	Array Status: • 0 = No Errors • 1 = Rebuilding • 2 = Ready to Rebuild • 3 = Recovery Made • 4 = Drive Fail • 5 = Unknown The letter *n* in the Attribute Code is an indicator of which Array, as some servers are attached to multiple arrays.	If the Array Status is not "No Errors" (0), check the reason. If it is either rebuilding or in recovery, wait for a period of time for the array to restore to normal state; if it persists contact HP technical support. If a drive has failed, replace the drive and allow time for it to rebuild. If the array is unknown or failed, check for error indicators. If the problem persists, contact HP technical support.

Attr. Code	Description	Recommended Action
PTE*n*	Temperature State; an indication of the temperature status, summarizing the RAID temperature situation: • 0 = OK • 1 = Temp Low • 2 = Temp High • 3 = Critical • 4 = Unavailable The letter *n* in the Attribute Code is an indicator of which RAID, as some servers are attached to multiple RAID units.	There may be some issues with the cooling around the servers, and measures should be implemented to help keep the servers cool or to investigate if the temperature is too low.
RMS1	RAID Monitor Status. This is an overall indication of whether the RAID monitor driver is connecting with the SSM service: • 0 = Connected • 1 = Connecting... • 2 = Disconnected A status of "Disconnected" does not mean that the RAID is faulty, only that the SSM is unable to monitor it.	If the monitor is "Disconnected" for an extended period, restart the server. If this does not clear the problem, contact HP technical support.
RSTU	FSG Replication status; whether the component is: • 0 = Normal • 1 = No Primary • 2 = Error	If the device reports "No Primary", ensure the primary FSG service of the replication group is online and running normally. If the status is "Error", contact HP technical support.
SAVP	Space Available; the percentage of storage space remaining on all object stores of the server. Adjusting the alarm threshold allows you to proactively manage when additional storage needs to be purchased.	If the available space is reaching a low threshold, you should start looking into either purchasing additional storage or migrating some data to archive, depending on your available options.

Attr. Code	Description	Recommended Action
SLSA	System Load Average; an indication of how busy the system is. The higher the value the busier the system. Typically above 10 should be investigated as it indicates a fairly high load on the system. Over 25 is considered a critical issue.	If the System Load Average persists at a high value, the number of transactions (seen by graphing network bandwidth usage) in the system should be investigated to determine whether this is due to heavy load at the time. If there does not appear to be a heavy load on the system, and the alarm persists, contact HP technical support.
SMST	Log Monitor; an indication of the status of the log monitoring within the SSM: • 0 = Connected • 1 = Initializing • 2 = Shutdown • 3 = Bad Configuration • 4 = Unable to Connect	If the Log Monitor has non-zero values persisting for a period of time, contact HP technical support.
SMTT	Total Events; the number of error events that have been logged by the SSM.	If the Total Events becomes non-zero, check if there are known events (such as RAID failures) that could have caused this. When an issue is resolved, the counter can be reset to zero as noted on page 142. If there have not been any known events in the SSM, or the number increases and the alarm persists, contact HP technical support.

Attr. Code	Description	Recommended Action
SPOP	FSG Pending Operations; indicates the number of replication messages to be processed by a Secondary FSG. If this rises, it indicates that you are storing data faster than the Secondary FSG can process transactions. This normally declines during periods of reduced grid activity. There is a warning at 500, and a minor alarm if more than 1000. *Note: this alarm may trigger during normal file system backup. Allow any active backup to complete, then monitor for a declining value.*	Stop storing files into the Primary FSG of the group. Wait a few minutes to determine if the value of this attribute declines. When the alarm clears, resume normal activity on the Primary FSG. If the value does not decline, contact HP technical support.
SSMA	SSM Device Status; indicates the general status of the SSM service: • 0 = No errors • 10 = Errors	If there is an Error, check the Overview and Alarm tabs for the device to find the cause of the error and to troubleshoot the problem. If the problem persists, contact HP technical support.
SSME	SSM Device State; whether the device is: • 0 = Offline • 1 = Standby • 2 = Online	If the device goes into “Standby”, continue monitoring and if the problem persists, contact HP technical support. If the device goes into “Offline” and there are no known server hardware issues (server unplugged) or a scheduled downtime for the device, contact HP technical support.

Attr. Code	Description	Recommended Action
SSTE	Storage State; an indication of the current status of the component: • 0 = Offline • 1 = Standby • 2 = Verify • 3 = Online (Read-Only) • 4 = Online If the Storage State goes into Verify, this means it is running through the data and verifying its data integrity; a normal operation. If the state is Online (Read-Only) new data cannot be stored into this LDR, but data can be requested and viewed. Standby state is a minor alarm. This is usually a transitory state used to step between online and offline or verify.	If the Storage State is in "Verify", this may be normal operation and may take quite some time depending on the quantity of data. If it continues over two days however, contact HP technical support. If the Storage State is "Offline", it can be brought Online again using the Configuration tab for that device or component.
SSTU	Storage Status; an indication of the status of the storage component: • 0 = No Errors • 1 = Not Started • 2 = Performing Startup Checks • 3 = Inaccessible • 4 = Crosscheck Failed • 5 = Corrupt • 6 = Verify Location Synchronize Failed • 7 = Maximum number of failures reached • 8 = Insufficient Free Space • 9 = Unknown Error	If the Storage Status has "Insufficient Free Space", there is no more available storage on the server; data ingests are redirected to other available nodes. Viewing requests can continue to be delivered from this node. Additional storage should be added to this server. It is *not* impacting end user functionality, but the alarm persists until additional storage is added. If Storage Status is any other error condition, contact HP technical support.
SVST	Service Status; the status of the services component of the SSM: • 0 = Not Running • 2 = Running	This alarm clears when other alarms related to a non-running service are resolved. Track the source service alarms to restore operation.

Attr. Code	Description	Recommended Action
SWMU	System Swap Memory Used; measured in bytes. Values less than 100 MB are considered normal; over 500 MB is a major issue.	If a service is persistently using large amounts of the virtual memory swap storage, upgrade the amount of RAM in the server.
TNER	Network Neighbor Drift; an indication in µs of how far the clock is drifting should it become disconnected from a GPS system. Absolute values more than 1,000,000 (1 s) are a minor issue. Twice that is considered a major issue. If *slow* by 2 s, the situation could be critical.	If the drift becomes large either in the positive or negative direction, this should be investigated immediately, contact HP technical support.
TRFS	Reference Clock; an indication of the status of the reference clock: • 0 = Stable • 1 = Flywheeling • 2 = Unstable • 3 = Offline • 4 = Unknown	If the reference clock starts flywheeling, this means it is drifting and there is no way to determine the accuracy of the clock. If this occurs, check the connections with the GPS, and if it persists, contact HP technical support. If it then becomes “Unstable”, “Offline” or “Unknown”, contact HP technical support *immediately*.
TRSS	Local Clock Status; an indication of the status of the local clock: • 0 = Calibrating • 1 = Synchronizing • 2 = Syntonizing • 3 = Flywheeling (Recalibrating) • 4 = Flywheeling Only “Flywheeling” is considered problematic.	If the local clock starts flywheeling, contact HP technical support.
UMEM	Utilized Memory; the amount of system RAM (in MB) *remaining available* for system operations. Anything over 100 MB is considered normal. Below 50 MB is a major issue; below 10 MB is critical.	If the available RAM gets fairly low, it needs to be investigated as to whether this is a hardware or software issue. If it is determined not to be a hardware issue, or if it falls below 50 MB, contact HP technical support *immediately*.

Attr. Code	Description	Recommended Action
VMFI	Volume Free entities; a measure of how many more objects the volume can store. Values below 100,000 start to raise a concern. When the value dips below 25,000 the situation is a major issue that should be addressed. Values below 10,000 are considered critical.	This is an indication that additional storage is needed on the server. Contact HP technical support for assistance in installing and configuring new object storage.
VMFR	Volume Free Space; the amount of free space still available (in bytes) on the server. Concern is not raised until the free space falls below 1 GB. At 100 MB the situation is considered major. Values below 10 MB are a critical concern.	If the Free Space gets fairly low, it needs to be investigated as to whether there are log files growing out of proportion, or files taking up too much memory that need to be reduced or deleted. If this problem persists, contact HP technical support.
VMST	Volume Status; an indication of the status of the volume on the server: • 0 = Unknown • 1 = Offline • 2 = Online	If the Volume Status indicates “Offline”, contact HP technical support.

Introduction to Server Manager

8

Essential background to understanding Server Manager.

Chapter Contents

Overview of Server Manager 196
Services 196
Capabilities 197

Architecture Overview 197
The Core Application 197
Automatic Startup and Shutdown 198

Overview of Server Manager

Each server used in an HP Medical Archive deployment runs the Server Manager application. The Server Manager program is used to supervise starting and stopping services on the server, ensuring services gracefully join and leave the grid. It also monitors services on the server, and attempts to restart any that report faults.

Grid services have a variety of dependencies on support packages such as networking, timing synchronization, and third-party programs such as databases. Server Manager ensures that these support services are brought online in the correct sequence to meet dependencies.

Server Manager provides you with a graphical interface on the local console of the server, enabling coarse (whole server) control and monitoring of the device. The state of services is reported, along with server identity information such as IP addresses. Control buttons allow you to stop services to perform upgrades, reboot the server, or shut the server down for hardware maintenance. All operations preserve graceful service disconnections and restarts; grid operations are smoothly completed before the services are removed from the grid. Services and support applications are stopped in a sequence that avoids breaking any interdependencies.

Server Manager continues to run at all times, monitoring the services and automatically restarting any that go offline. Should a service go offline unexpectedly or a server suffer an unexpected power cycle or reset, Server Manager ensures all services are brought back online without the need of manual intervention.

Services

The first part of this manual (dealing with the NMS) uses specific terminology for locations, servers, services, and so on. This discussion of the Server Manager refers to “services” in a broader sense, including operating system processes such as networking and file systems and third-party modules such as the MySQL database application. Where reference to only the grid services is needed, the word “grid” is always used.

Capabilities

Server Manager provides the following capabilities:

- Stop and start all services on a server for:
  - Restarting grid services that have gone offline
  - Stopping the services in preparation for an upgrade
  - Bringing up the services after a reconfiguration
- Detect OS shutdown and gracefully close services.
- Restart a server; bring down everything, including the OS, and reboot the machine from the BIOS up.
- Shutdown a server to the point where it must be manually restarted. This enables you to safely power down a server for hardware maintenance.
- Automatically start services if the server is power cycled or reset, and to recover from unintentional restarts.
- Monitor services on an ongoing basis and restart them as needed.

Architecture Overview

Server Manager is implemented in two parts: a core application and a Graphical User Interface (GUI). The core application is intended to run tightly coupled with the operating system so that it is always available to manage the server. The GUI is run separately, offering administrators a graphical local console for monitoring the server, rather than the operating system's command line interface.

The Core Application

At installation, Server Manager is configured to automatically start with the operating system. It is always running and available, intended to be left unattended.

The core application provides the logic to:

- Sequentially verify and start the services to bring the server up and gracefully connect to the grid.
- Sequentially stop services to gracefully disconnect from the grid.
- Monitor grid services to restart services that go offline.
- Automatically restart services if the server is restarted or power cycled.
- Respond to commands from the GUI interface.

Server Manager is designed to run whenever the server is running.

Automatic Startup and Shutdown

During system startup, Server Manager is automatically started by the operating system. Server Manager executes a sequential series of scripts to verify that support services are running, and start them as needed. The startup and shutdown sequences are reversed, ensuring that dependencies are in place as needed, and are not removed prematurely.

The GUI interface to Server Manager is one of the services started through this sequence of scripts. It is placed early in the sequence so that it can report the status of other services as they startup or shutdown.

Server Manager Operation

9

Using the Local Console

Chapter Contents

Display Components 200
- Header 200
- Service List 201
- Control Buttons 202
- Server Identification 202
- Prompt Line 203

Using the Interface 203
- Display Updates 203
- Keyboard Input 203

Command Operations 204
- Monitoring Services 204
- Starting Services 205
- Stopping Services 205
- Restarting the Server 205
- Shutting Down the Server 206

Display Components

The Server Manager presents a Graphical User Interface (GUI) on the local console of the server. The display uses five panels to present information and controls.

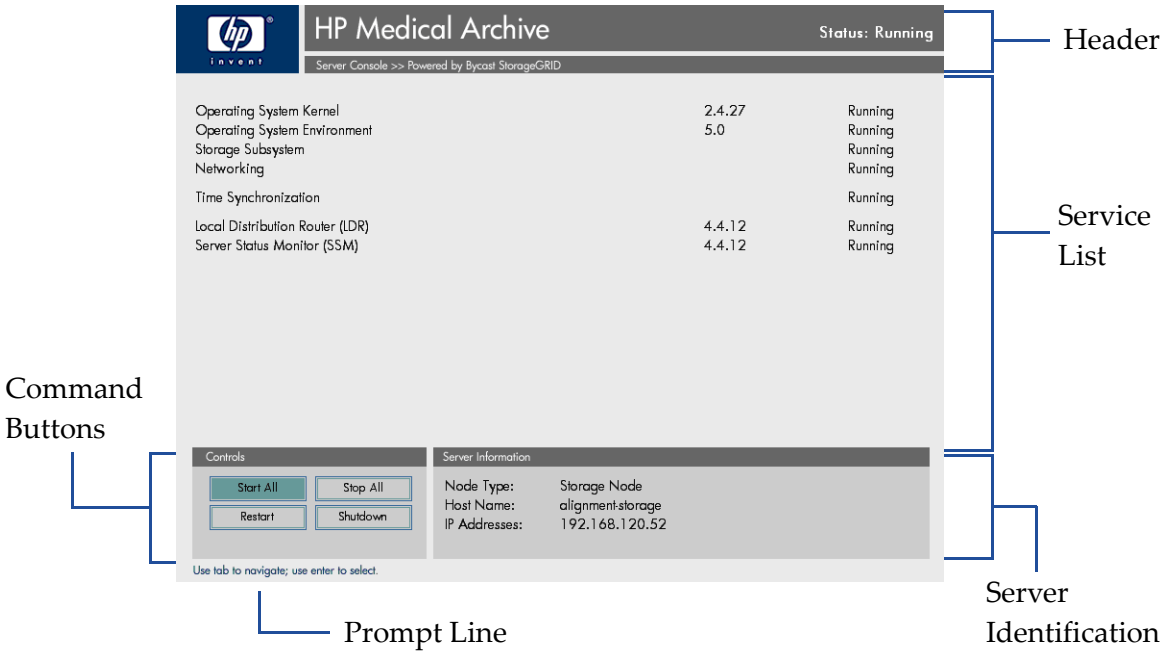


Figure 30: Server Manager Interface Sample

Header

The top of the screen presents a header line, identifying the Server Manager application and its overall status.

When running normally, the top line appears with a dark grey background, matching the background of the rest of the screen. If *any* of the services is reporting an error, the background changes to red to draw immediate attention.

Status

The status line is an aggregate representation of the state of the services under its control. If they are all stopped, the status is "Stopped"; all running, "Running", and so on. However, if *any* of the

services are in an error state, the Status reports "Error", and the header background turns red.

Service List

The body of the display is a list of the services being monitored by the Server Manager.

Service Name

The name of each service is shown. For grid services, the names are the fixed service names.

Some services may appear that are not identified through the NMS. These are services that can run independently and provide support capabilities to the grid services.

Version

Where a version number is available from the service, it is displayed in the list. This provides a quick reference for administrators to verify the currency of services and identify if updates are required.

Status

Nominally these all report "Verified" or "Running". As the services are being started or stopped, the status may report the transition stage, such as "Stopping..." or "Starting...". Additionally, "Stopped" indicates a service that has been ordered stopped by the Server Manager and will not restart without a Server Manager command.

If a grid service reports an error state, the status reported here indicates "Error" and the Server Manager header changes to a red background. Server Manager attempts to recover the service up to three times. If the service remains in error state—without recovery to a "Running" state—after three consecutive retries, Server Manager monitors and reports the state but does not continue automatic attempts to restart it.

Control Buttons

Located in the bottom left corner are four control buttons used to stop and start services and reboot or halt the server. Use of these command buttons ensures the services enter and leave the grid gracefully.

The currently selected button is shown with a yellow box around the button text.

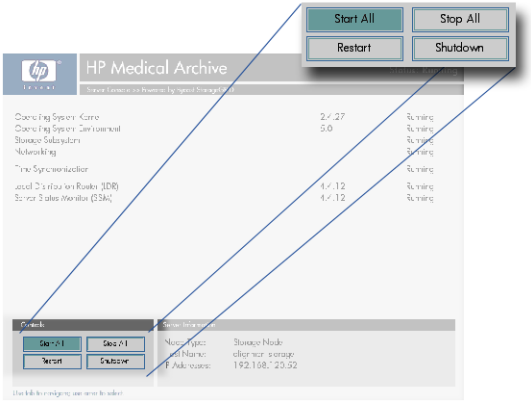


Figure 31: Sample Selected Button

Use of these buttons is described in detail in “Command Operations” on page 204.

Server Identification

The bottom right portion of the display provides information about the server itself.

Node Type

This name is allocated at installation to describe the type of grid services hosted on the server, such as “Control Node” or “Storage Node”.

Host Name

This is the name of the server as specified in the original installation configuration file.

At the time a deployment is configured, a file is prepared that identifies each server and the services it hosts. This file is used to generate

the installation disks. The server name used in that file is reported by Server Manager as the Host Name.

IP Addresses

The server's operating system networking service is used to report the IP addresses assigned to the network interface(s). Most servers have only one address; however, if multiple adapters/addresses are available, all are reported.

Prompt Line

At the very bottom of the display is a prompt line, providing guidance on what actions you can take. This typically states: "Use tab to select the button, and enter to activate it." See "Control Buttons" on page 202 for more on using the buttons.

Using the Interface

Display Updates

The display of service states is updated on a timed poll, every ten seconds. If the core application of the Server Manager detects an event, an asynchronous update is possible.

Keyboard Input

The interface only supports use of the command buttons shown in the bottom left of the display. These are selected and activated using the <Tab> and <Enter> keys. A confirmation is required for all actions.

Response Time

Note that input from the keyboard is registered with the application on a polling cycle, which means that there may be a delay of a few seconds before your keystroke is shown on the display. Keystrokes are buffered and queued.

Ensure that you see the result of a <Tab> keystroke *before* pressing the <Enter> key to activate the selection. Pressing <Tab> repeatedly while

waiting for the display to “catch up” may result in activating the wrong command.

Initiating an Action

To initiate an action:

1. Press the **<Tab>** key to cycle the highlight to the desired control button. Each press cycles to the next button in a standard rotation.
2. Press **<Enter>** to indicate that you want to initiate the selected action.

   A confirmation dialog opens allowing you to confirm or cancel the action.
3. Use the **<Tab>** key to select **OK** (confirming the action) or Cancel. A highlight box is used to show the current selection.
4. Press **<Enter>** to complete the input, either initiating the action or cancelling it.

   The dialog closes and Server Manager returns to normal operation, either executing the action (OK) or waiting for another command button selection (Cancel).

Command Operations

Monitoring Services

While running normally, the Server Manager is constantly monitoring the services (at ten second intervals). If a service is taken offline or fails, the Server Manager attempts to restart it.

Attempts to restart a stopped service are persistent; that is, as long as the service is not running, the Server Manager continues to issue restarts indefinitely.

An error state in a running service is handled differently than an offline service. Server Manager attempts to restart the service up to three times. If it remains in an error state, Server Manager continues to monitor the service but does not persist in automatic restart attempts.

Starting Services

This button is used to start services that have been stopped for upgrade or other configuration changes.

Upon server startup, or when commanded via the **Start All** button, the Server Manager executes a series of scripts to initiate dependent applications in a sequence that ensures prerequisite services are running before starting the grid services themselves.

The operating system kernel, environment, and hardware services for storage and networking are verified first. Following the operating system services, time synchronization is verified. This process can take several minutes while the system characterizes and builds trust in the time signal source.

Any third-party applications required to support the grid service software on the server are started, if not already running.

Finally the HP Medical Archive services are started and the server joins the grid. Any services already running are not disrupted.

Stopping Services

The command button to **Stop All** can be used to gracefully stop services hosted on this server, effectively disconnecting it from the grid. The operating system and Server Manager continue to run on the server, allowing you to perform tasks such as configuration changes, software updates, and similar maintenance that requires the operating system. Grid services and third-party applications are stopped.

When maintenance tasks are finished, you can either:

- **Start All** services to gracefully start the grid services and rejoin the grid (page 200).

  — or —
- **Restart** the server; bootstrapping the operating system and then starting grid services (below).

Restarting the Server

This command gracefully stops the grid services, and also brings down the operating system to perform an automatic reboot. This is useful for resetting a server that has failed, or starting a new configuration.

The Server Manager performs the same sequence as the Stop All command (page 205), then continues to bring down the operating system. The Server Manager and GUI are closed by the operating system as part of its shutdown.

Settings in the operating system are used to trigger a reboot, which in turn restarts the Server Manager application. Server Manager then restarts the GUI and all services.

Shutting Down the Server

If the server must be powered down for hardware maintenance, upgrades, or reconfiguration, this command should be used. Similar to Restart, this gracefully closes services and halts the operating system. Unlike Restart, this command does not trigger a reboot. The system is fully halted, requiring a power cycle or hardware reset to restart the server and operating system.

The Server Manager performs the same sequence as the Stop All command (page 205), then continues to bring down the operating system to a halted state. The Server Manager and GUI are closed by the operating system as part of its shutdown.

When a server is restarted, the Server Manager application is automatically restarted and resumes normal operation, restarting all services.

Glossary

ADC Administrative Domain Controller—a unit of the HP Medical Archive software that authenticates grid nodes (certificates) and manages interconnections. It maintains grid topology information.

ADG Advanced Data Guarding—HP proprietary fault tolerance mechanism implemented in certain models of HP "Smart Array" RAID storage. Two sets of parity data are distributed across all drives to protect against the failure of any two drives in an array.

AE title Application Entity Title—the identifier of a DICOM node communicating with other DICOM AEs.

AMS Audit Management System—a unit of the HP Medical Archive software that monitors and logs all audited system events and transactions.

CBID Content Block Identifier—A number that uniquely identifies a piece of content within the HP Medical Archive system.

CIDR Classless Inter-Domain Routing—a method of routing traffic between IP networks that improves flexibility when dividing ranges of IP Addresses into separate networks. CIDR is defined in RFC 1519. Standard notation for a CIDR address range begins with the network address, padded with zero bits on the right, followed by a slash "/" character and a number representing the length in bits of the subnet mask (*prefix*), thus defining the size of the network. For example:

- 192.168.120.0/24 represents the 256 addresses 192.168.120.0 through 192.168.120.255 inclusive. The "/24" indicates a 24-bit subnet mask, leaving 8 bits (0–255) of subnet address space.
- 192.168.212.0/22 represents the 1024 addresses 192.168.212.0 through 192.168.215.255 inclusive. The left-most 22 bits form the mask, leaving 10 bits (0.0–3.255) of subnet address space.

CIFS Common Internet File System—a file system protocol based on SMB (Server Message Block, developed by Microsoft) intended to complement existing protocols such as HTTP, FTP, and NFS.

CLB Connection Load Balancer—a unit of the HP Medical Archive software that directs incoming DICOM traffic based on factors from an ADC.

CMN Configuration Management Node—a unit of the HP Medical Archive software for performing system-wide reconfiguration and Grid Tasks.

CMS Content Management System—a unit of the HP Medical Archive software managing a distributed database catalog of the grid content (metadata) and data duplication according to business rules to provide Information Lifecycle Management (ILM).

content block ID See "CBID".

DICOM Digital Imaging and COmmunications in Medicine—a standard developed by ACR-NEMA (an alliance of the American College of Radiology and the National Electrical Manufacturer's Association) for communications between medical imaging devices.

DR Disaster Recovery.

FCS Fixed Content Storage—A class of stored data where the data, once captured, is rarely changed and must be retained for long periods of time in its original form. Typically this includes images, documents, and other data where alterations would reduce the value of the stored information.

flywheeling A clock is running on its own, without tracking a reference source.

FSG File System Gateway—a unit of the HP Medical Archive software that enables standard network file systems to interface with the grid.

Grid Task A managed sequence of actions that are coordinated across a grid to perform a specific function (such as adding new node certificates). Grid Tasks are typically long-term operations that span many entities within the grid.

HPMA HP Medical Archive—a fixed-content storage system from Hewlett-Packard. The solution is sold under the HP brand and is serviced and supported by the HP services/support organization worldwide. The HPMA Solution is powered by Bycast® StorageGRID™ software.

ILM Information Lifecycle Management—a process of managing data by applying business rules to determine storage accessibility and longevity. Software implementing ILM manages data replication, storage resources, distribution, and retention to meet business and regulatory objectives.

instance A DICOM term for an image. One or more instances for a single patient are collected in a "study".

LAN Local Area Network—a network of interconnected computers that is restricted to a small area, such as a building or campus. A LAN may be considered a node to the Internet or other wide area network.

latency Time duration for processing a transaction or transmitting a unit of data from end to end. When evaluating system performance, both throughput and latency need to be considered. See also: “throughput”.

LDR Local Distribution Router—a unit of the HP Medical Archive software to manage the storage and transmission of content within the grid.

metadata Data that provides information *about* other data.

namespace A set whose elements are unique names. There is no guarantee that a name in one namespace is not repeated in a different namespace.

NFS Network File System—a protocol (developed by SUN Microsystems) that enables access to network files as if they were on local disks.

NMS Network Management System—a unit of the HP Medical Archive software for alarm monitoring and system administration. It provides a web-based interface for managing and monitoring the HPMA system, as well as viewing and reporting on statistics regarding network, DICOM, storage, and many other related attributes for each of the various services and servers.

object store A configured file system on a disk volume. The configuration includes a specific directory structure and resources initialized at system installation.

PACS Picture Archiving and Communication System—a computerized system of patient records management responsible for short and long term (archival) storage of images. Communication with PACS is via DICOM.

PDF Portable Document Format—a file format (developed by Adobe Systems and based on the postscript language) for exchanging documents between computer systems that may have differing operating systems. It is designed to preserve the appearance of the document regardless of the system used to render it.

release The edition of the complete HP Medical Archive system. Contrast with “version” and “revision”.

revision The edition of a document. Contrast with “version” and “release”.

Samba A suite of programs that implement the Server Message Block (SMB) protocol. It allows files and printers on the host operating system to be shared with other clients. For example, instead of using telnet to log into a Unix machine to edit a file there, a Windows user might connect a drive in Windows Explorer to a Samba server on the Unix machine and edit the file in a Windows editor.

SATA Serial Advanced Technology Attachment—a standard for connecting hard disks into computer systems. As its name implies, SATA is based on serial signaling technology, unlike IDE (Integrated Drive Electronics) hard drives that use parallel signaling.

SQL Structured Query Language—an industry standard interface language for managing relational databases. An SQL database is one that supports the SQL interface.

SSM Service Status Monitor—a unit of the HP Medical Archive software that monitors hardware conditions and reports to the NMS. Every server in the grid runs an instance of the SSM.

StorageGRID™ A trademark of Bycast Inc. for their fixed-content storage grid architecture and software system.

study A DICOM term for a collection of images (instances) related to an individual patient or subject.

SVG Scalable Vector Graphic—a format for digital images that can be scaled without loss of resolution.

synchronizing A clock is running at the same pace and at the same time (value) as a reference source.

syntonizing A clock is running at the same pace as a reference source, but not necessarily reporting the same time.

TCP/IP Transmission Control Protocol / Internet Protocol—a process for encapsulating and transmitting packet data over a network. It includes positive acknowledgement of transmissions.

throughput The amount of data that can be transmitted or the number of transactions that can be processed by a system or subsystem in a given period of time. See also: “latency”.

URI Universal Resource Identifier—A generic set of all names or addresses used to refer to resources that can be served from a computer system. These addresses are represented as short text strings.

URL Universal Resource Location—A URI that can be typed into a browser or other client program in order to retrieve/access an object, such that the client software is able to understand how to perform the requested action. (The client, typically a “browser”, often uses a Domain Name Server (DNS) to resolve a URL into an IP address and URI combination.)

UTC A language-independent international abbreviation, UTC is neither English nor French. It means both “Coordinated Universal Time” and “Temps Universel Coordonné”.

UTC refers to the standard time common to every place in the world. It is derived from International Atomic Time (TAI) by the addition of a whole number of “leap seconds” to synchronize it with Universal Time (UT1). UTC is expressed using a 24-hour clock and uses the Gregorian calendar.

UUID Universal Unique IDentifier—A 128-bit number which is guaranteed to be unique.

version The edition of a service within the HP Medical Archive system. Contrast with “release” and “revision”.

WAN Wide Area Network—a network of interconnected computers that covers a large geographic area such as a country. Contrast with LAN.

Index

A
accessing NMS 5
accounts, user *See* user account
ADC
  configuration 159
  service 56–60
alarms
  active 18, 155
  attribute codes 172–193
  clearing 35
  configuration 153–157
  handling 34–35
  history page 32–34
  indicators 28
  levels 26, 28
  main page 31–32
  monitoring 26–28
  notification 27
  propagation 28, 29
  queries 32
  tab 19, 30
  table headings 31
AMS
  configuration 160
  service 61–66
architecture, HPMA 2
architecture, Server Manager 197–198
attributes
  alarm codes 172–193
  interpreting tables 54
  network element 4
audit messages
  access 80
  configuration 162
  levels 80

B
backup, FSG 110
browser, requirements 5
bytes, interpretation 55

C
cabinet map 21
CBID, definition 207
charts 42–44
  bar graph 44
  interpreting 43
  level graph 43
  printing 46
  state graph 44
  view controls 45
CIDR, definition 207
CIFS 112
CLB
  configuration 160
  service 67–75
clearing alarms 35
client services 112
CMN
  configuration 161
  service 76–93
CMS
  configuration 162
  service 94–101
color, of text 18
components
  list of 52
  network element 4
configuration
  ADC 159
  alarms 153–157
  AMS 160
  audit messages 162
  CLB 160
  CMN 161
  CMS 162
  common service attributes 158–159
  FSG 162
  LDR 164–167
  main page 158
  NMS 168
  notification page 153
  permissions 152
  SSM 168–170
  tab 19
  warnings 152
contacts xiv
content frame 16
  pages 17
  tabs 16
conventions
  fonts xiii
  numeric xiii
  terminology xii
cookies 5
custom reports 41

D
DICOM
  metadata tag index 88
duration, interpretation 55

F
flywheeling, definition 208
frames 12–20
  content 16
  header 12
  navigation tree 15
  Server Manager 200–203
FSG
  backup status 110
  client services 112
  configuration 162
  replication groups 88
  replication status 108
  service 102–114

G
grid
  ID number 89
  options 89
grid node (definition) xiii
Grid Tasks
  status 89

H
header frame 12
host name 202
HPMA
  architecture 2

I
ID number, grid 89
immediate reports 39
indicators
  alarms 28
  immediate report 39
  in navigation tree 16
  system status 14
interpreting charts 43
IP addresses, of server 203

J
javascript 5

L
languages 91
LDR
  configuration 164–167
  service 115–131
level, alarm 28
location map 21
locations, network element 3
log in 6
log out 6

M
maps 21–23
metadata
  definition 209
  DICOM 88
monitoring alarms 26–28

N
namespace, definition 209
navigation tree 15
  sequence 91
network elements
  attributes 4
  components 4
  locations 3
  nodes 3
  services 4
NFS 112
NMS
  accessing 5
  configuration 168
  role of 3
  service 132–137
NMS Entities, CMN component 91
node (definition) xiii
node maps 22
node type 202
nodes, network element 3
notifications 27
numeric conventions xiii

O
object store, definition 209
overview tab 17

P
pages, in content frame 17
password 5
  changing 10
  forgotten 6
permissions
  user account 7
printing reports 46

Q
quick reports 40

R
RAID, SSM component 146
refresh 13
release
  definition 209
  number ix
replication (FSG)
  groups 88
  status 108
reports
  accessing 39
  bar graph 44
  chart view controls 45
  charts 42–44
  custom 41
  formats 42–45
  immediate 39
  interpreting charts 43
  level graph 43
  printing 46
  quick 40
  state graph 44
  tab 19
  text 44
restarting server (Server Manager) 205
revision
  definition 209
  number ix

S
Server Manager
  GUI 200–203
  operations 204
  role of 196
services
  ADC 56–60
  AMS 61–66
  CLB 67–75
  CMN 76–93
  CMS 94–101
  FSG 102–114
  LDR 115–131
  list of 50
  map 22
  network element 4
  NMS 132–137
  SSM 138–149
shutting down server (Server Manager) 206
sites 3
SSM
  configuration 168–170
  service 138–149
starting services (Server Manager) 205
stopping services (Server Manager) 205
SVG
  definition 210
  viewer 5
synchronizing, definition 210
syntonizing, definition 210
system requirements 5
system status indicator 14

T
tabs
  alarms 19, 30
  configuration 19
  in content frame 16
  overview 17
  reports 19
terminology
  conventions xii
  network elements 3
text color 18
text reports 44
tree, navigation 15
troubleshooting
  alarm handling 34
  attribute codes 172–193

U
URI, definition 210
URL, definition 210
user account
  accessing 14
  permissions 7–10, 152
user name 5
  changing 10

V
version
  definition 211
  finding NMS 14
  number ix
  reported by Server Manager 201